PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

PCT / FI03 / 00664

Helsinki 31.10.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija / Applicant: **Talvitie, Jarmo, Tuusula**

Patenttihakemus nro / Patent application no: **20021635**

Tekemispäivä / Filing date: **12.09.2002**

Kansainvälinen luokka / International class: **G06F**

Keksinnön nimitys / Title of invention:

"Turvajärjestelmä, menetelmä ja laite tietokonevirusten torjumiseksi, sekä tiedon eristämiseksi"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kalla
Tutkimussihteeri

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Turvajärjestelmä, menetelmä ja laite tietokonevirusten torjumiseksi sekä tiedon eristämiseksi

Ett skyddsystem, ett förfarande och en anordning för att avvända datorvirus och isolera information

Keksintö liittyy tietokoneisiin, tietoverkkoihin ja tietoliikennejärjestelmiin, ja erityisesti niissä esiintyvien virusten torjuntaan.

Tietokoneissa esiintyvät virukset ovat ohjelmanpätkiä, joiden pääasiallisena tarkoituksena on levittäytyä eteenpäin. Monet virukset aiheuttavat lisäksi joko tarkoituksellisesti tai tahattomasti vahinkoa isäntäkoneissa, joissa ne ovat aktivoituneet. Virukset saattavat viestiä itsestään tulostamalla tietokoneen näyttölaitteelle viestejä tai tuhoamalla tiedostoja. Virus on tavallisimmin kiinnittyneenä yhteen tai useampaan tiedostoon ja aktivoituu kyseistä tiedostoa avattaessa tai tiedoston ollessa ohjelma, sitä käynnistettäessä. Aktivoitumisen jälkeen virus voi kiinnittyä muihin tiedostoihin, ilmoittaa itsestään koneen käyttäjälle tai tuottaa vahinkoa mm. tuhoamalla työ- tai massamuistin sisältöä. Ennen Internetin aikakautta virukset levisivät tyypillisesti levykkeiden välityksellä laitteesta toiseen. Nykyisin virusten saastuttamien tiedostojen lataaminen Internetistä tai viruksia sisältävien sähköpostiviestien avaaminen ovat yleisimpiä tartunnan lähteitä. Laajat tietoverkot kuten Internet ovat mainioita ympäristöjä virusten laajamittaista levitystä silmälläpitäen, sillä virusten alkuperäisen levittäjän jäljittäminen on verkon dynaamisen ja osittain käyttäjien anonymiteettiakin suojaavan luonteen takia hankalaa, ja toisaalta potentiaalisia tartunnansaajia on lähes rajattomasti ympäri maailman.

Useimmiten varsin yleisluontoisesti käytetyn viruskäsitteen alta voidaan erottaa myös alaluokkia kuten madot ja troijalaiset hevoset. Madot ovat ohjelmia, jotka pystyvät leviämään itsenäisesti ilman käyttäjän suorittamia viruksen kannalta edullisia toimenpiteitä, joita perinteisten virusten aktivoiminen tavallisesti vaatii. Madot hyödyntävät esim. automaattisia tiedostojen lähetys/vastaanotto-ominaisuuksia, joita on integroitu nykyaikaisiin tietokoneisiin ja tietokonejärjestelmiin. Termin "troijalainen hevonen" käyttö pohjautuu nimensä mukaisesti antiikin Kreikassa suoritettuun klassiseen petokseen ja antaa vihjeen kyseisen nimityksen saaneen ohjelman petollisesta luonteesta. Troijalainen hevonen on ohjelma, joka on naamioitu joksikin muuksi, useimmiten joko hyötykäyttöön tai pelkäksi ajanvietteeksi tarkoitetuksi ohjelmaksi. Troijalainen hevonen voi lisäksi sisältää perinteisten virusten tai matojen piirteitä. Osa viruksista voi myös kiinnittyä tavallisten tiedostojen lisäksi tietoko-

neen massamuistissa, joko kovalevyllä tai levykkeellä, sijaitsevaan käynnistyssektoriin. Nämä virukset aktivoituvat tyypillisesti välittömästi tietokoneen käynnistyksen yhteydessä tai levykkeen sisältöä luettaessa. Virukset saattavat toisaalta pystyä peittelemään olemassaoloaan tarkkailemalla tietokoneessa suoritettuja systeemikutsuja, joissa käsitellään esim. massamuistin muistilohkoja, ja palauttaa kutsujasovellukselle muistilohkojen alkuperäisen, talteen otetun, sisällön niiden nykyisen, viruksen muunteleman, datan sijaan.

Niin perinteisiä viruksia, matoja, troijalaisia hevosia kuin näiden yhdistelmiäkin vastaan voidaan suojautua useita, keskenään varsin erityyppisiä menetelmiä hyödyntämällä. Tietokoneisiin asennettavia virustentorjuntaohjelmia ajetaan useimmiten jatkuvasti ns. tausta-ajona ja ne sijoitetaan ainakin osittain tietokoneen käynnistyksen yhteydessä työmuistiin valvomaan dataliikennettä tietoverkon ja siihen liitetyn tietokoneen välillä, koneen omia sisäisiä operaatioita ja ainakin välillisesti myös massamuistin sisältöä. Tietokoneen sisäiset operaatiot liittyvät esim. muistin ja tiedostojen käsittelyyn sekä oheislaitteiden ohjaamiseen. Torjuntaohjelmat sisältävät yleensä tietokannan tunnettujen virusten niistä piirteistä, ns. sormenjäljistä, jotka ovat kullekin virukselle tai virustyypille ominaisia. Kun tietokoneen työmuistiin ladataan uusi tiedosto, esim. ohjelma, koneen muistissa oleva torjuntaohjelmisto suorittaa haun, jossa verrataan tunnettujen virusten piirteitä kyseisen tiedoston sisältämään informaatioon.

Tärkeät tiedostot voidaan erikseen suojata esim. CRC (Cyclic Redundancy Check) - tai ns. "hash" -tarkisteita käyttäen. Mikäli tiedostosta laskettu tarkiste ei vastaa alkuperäistä, virus on mahdollisesti kiinnittynyt tiedostoon ja muuttanut sen sisältämää informaatiota.

Klassisen virustentorjuntaohjelmiston tietokanta on aina päivitettävä sisältämään uudelle virukselle ominaiset tunnusmerkit ennen kuin virus voidaan luotettavasti havaita ja tunnistaa. Ns. monimuotoiset (polymorphic) virukset pystyvät muuntelemaan itseään kopioinnin yhteydessä ja niitä on siten erityisen hankala havaita perinteisiä torjuntaohjelmia käyttämällä. Monimuotoisen viruksen mutaatiot voivat sisältää samat toimenpiteet erilaisin käskysarjoin toteutettuina, jolloin viruksen toiminta säilyy ennallaan, mutta sormenjälkipohjaiset virustentorjuntaohjelmat eivät enää luotettavasti pysty tunnistamaan eri variaatioita viruksiksi. Toisaalta vaikka kaikki mahdolliset virustyypit sekä niiden mutaatiot voitaisiinkin tunnistaa, tunnusmerkkien tallentamiseen vaadittava tila ja vastaavasti niiden etsimiseen kuluva aika paisuisivat nopeasti kohtuuttomalle tasolle.

Julkaisussa US5889943 esitetään järjestelmä, jossa suljettu tietoverkko on yhdistetty ulkoiseen verkkoon yhdyskäytävän avulla. Yhdyskäytävä tutkii ulkoisesta verkosta tulevan ja toisaalta sinne lähtevän viestiliikenteen mahdollisten virustartuntojen varalta. Suljetun verkon sisäistä liikennettä ei tarkasteta. Julkaisussa esitetään myös erillinen laite käyttäjän koneeseen asennettavaksi. Laite sisältää tiedusteluyksikön (polling module) verkon yhteisessä postipalvelimessa (postal node) sijaitsevien uusien viestien havaitsemiseksi, vastaanottoyksikön (retrieval module) viestien vastaanottamiseksi postisolmulta ja analyysi/käsittely-yksikön (analysis/treatment module) virusten löytämiseksi viesteistä.

Keksinnön tavoitteena on välttää edellä mainituissa perinteisissä virustentorjuntamenetelmissä ja -järjestelmissä esiintyviä heikkouksia uudenlaisen turvajärjestelmän, siinä suoritettavan menetelmän ja uudenlaisen laitteen avulla.

Keksinnön mukaiselle turvajärjestelmälle virusten torjumiseksi tietokoneissa ja –verkoissa, joka turvajärjestelmä on järjestetty välittämään viestejä, on tunnusomaista, että se käsittää ensimmäisen alijärjestelmän tuntemattomien virusten havaitsemiseksi.

Keksintö koskee myös turvajärjestelmää tiedon eristämiseksi ensimmäisen ja toisen järjestelmän välillä, jolle turvajärjestelmälle on tunnusomaista, että se sisältää ensimmäisen ja toisen alijärjestelmän, ja se on järjestetty siirtämään tietoa ensimmäisen ja toisen järjestelmän välillä ensimmäisen ja toisen alijärjestelmän kautta, joka turvajärjestelmä on järjestetty katkaisemaan yhteys ensimmäisen järjestelmän ja ensimmäisen alijärjestelmän välillä ennen yhteyden muodostumista ensimmäisen ja toisen alijärjestelmän välille, ja järjestetty katkaisemaan yhteys ensimmäisen ja toisen alijärjestelmän välillä ennen yhteyden muodostumista toisen alijärjestelmän ja toisen järjestelmän välille.

Lisäksi keksintö koskee menetelmää virusten torjumiseksi tietokoneissa ja -verkoissa, jolle menetelmälle on tunnusomaista, että se suoritetaan järjestelmässä sisältäen ensimmäisen alijärjestelmän viestien välittämiseksi ja virusten havaitsemiseksi, joka ensimmäinen alijärjestelmä on tiedonsiirron osalta eristettävissä muusta järjestelmästä, joka menetelmä sisältää vaiheet, joissa:

- tarkkaillaan järjestelmän toimintaa viruksen havaitsemiseksi,
- havaittaessa virus suoritetaan hälytys.

Lisäksi keksintö koskee menetelmää virusten torjumiseksi tietokoneissa ja -verkoissa, jolle menetelmälle on tunnusomaista, että se sisältää vaiheet, joissa:

- suoritetaan järjestelmässä ainakin yksi toimenpide viruksen aktivoimiseksi,
- tarkkaillaan järjestelmän toimintaa virusaktivoitumisen aikaansaaman tapahtuman havaitsemiseksi,
- havaittaessa virus suoritetaan hälytys.

Lisäksi keksintö koskee menetelmää tiedon eristämiseksi ensimmäisen ja toisen järjestelmän välillä, jolle menetelmälle on tunnusomaista, että se suoritetaan turvajärjestelmässä, joka sisältää ensimmäisen ja toisen alijärjestelmän, joiden alijärjestelmien kautta siirretään tietoa ensimmäisen ja toisen järjestelmän välillä, jolle menetelmälle on tunnusomaista, että se sisältää vaiheet, joissa:

- katkaistaan yhteys ensimmäisen järjestelmän ja ensimmäisen alijärjestelmän välillä,
- muodostetaan yhteys ensimmäisen alijärjestelmän ja toisen alijärjestelmän välille,
- katkaistaan yhteys ensimmäisen alijärjestelmän ja toisen alijärjestelmän välillä,
- muodostetaan yhteys toisen alijärjestelmän ja toisen järjestelmän välille.

Lisäksi keksintö koskee laitetta virusten torjumiseksi tietokoneissa ja -verkoissa, joka laite sisältää välineet tiedon tallentamiseksi ja käsittelemiseksi sekä välineet tiedon siirtämiseksi toisen laitteen kanssa, jolle ensiksi mainitulle laitteelle on tunnusomaista, että se on järjestetty vastaanottamaan viesti mainitulta toiselta laitteelta ja tarkistamaan mainittu viesti tuntemattomien virusten havaitsemiseksi.

Keksinnön edullisen suoritusmuodon mukaan muodostetaan turvajärjestelmä tietokonevirusten torjumiseksi, joka järjestelmä sisältää alijärjestelmät 1-3. Alijärjestelmä 1 on ns. "kuraeteinen", joka välittää viestiliikenteen ulkoisen järjestelmän ja alijärjestelmän 3, ns. käyttäjän järjestelmän, välillä. Turvajärjestelmään ulkopuolelta saapuva viestiliikenne, joka on tavallisesti suunnattu käyttäjille alijärjestelmään 3, lähetetään ensiksi alijärjestelmästä 1 "eteiseen" eli alijärjestelmään 2, josta se myöhemmin ohjataan alijärjestelmään 3. Alijärjestelmä 2 sisältää jokaista alijärjestelmän 3 osoitetta, esim. koneen verkkotunnusta tai käyttäjän sähköpostiosoitetta, vastaavan osoitteen, jonka kautta viestiliikenne siirtyy alijärjestelmien 1 ja 3 välillä. Alijärjestelmällä 1 on tieto siitä, miten alijärjestelmien 2 ja 3 osoitetieto on yhdistettävissä keskenään, jotta saapuva liikenne voidaan edullisesti välittää alijärjestelmän

3 osoitetta vastaavaan osoitteeseen alijärjestelmässä 2. Alijärjestelmästä 1 on myös suojattu yhteys alijärjestelmiin 2 ja 3. Alijärjestelmästä 3 ulkoiseen järjestelmään suuntautuva viestiliikenne voidaan kierrättää vastaavasti turvajärjestelmän alijärjestelmien 1 ja 2 kautta. Alijärjestelmä 1 sisältää ne alijärjestelmän 3 ohjelmat ja toiminnot, joita virus voisi jollakin tapaa hyödyntää. Lisäksi alijärjestelmä 1 sisältää sellaiset ohjelmat ja toiminnot, jotka ovat perusteltuja virusten löytämiseksi. Näitä ohjelmia ovat esim. virustentorjuntaohjelmat ja ohjelmat, joiden avulla virus voidaan saada aktivoitumaan. Haluttaessa voidaan muitakin ohjelmia ja toimintoja, joita ei ole alijärjestelmässä 3, sisällyttää alijärjestelmään 1 sen suoritus- ja muistikapasiteetin asettamissa rajoissa. Alijärjestelmät 1-3 voidaan tarvittaessa liittää myös (ali)järjestelmään X, mikäli se virustentorjunnan kannalta katsotaan tarpeelliseksi. Jos alijärjestelmässä 1 tehdään virushavainto, lähetetään suojauskäsky alijärjestelmille 2 ja 3 suojattua yhteyttä pitkin. Viruksen aktivoituessa turvajärjestelmän alijärjestelmässä 1 sen aiheuttamat vahingot rajoittuvat alijärjestelmiin 1-2 estäen tai ainakin huomattavasti rajoittaen vahinkojen syntymistä alijärjestelmässä 3 tai muussa turvajärjestelmään liitetyssä, suojattavassa järjestelmässä, sillä alijärjestelmät on tiedonsiirron osalta mahdollista erottaa toisistaan tai muusta liitetystä järjestelmästä kuten ulkoisesta tietoverkosta esim. havaittaessa virushyökkäys.

Verkkoympäristössä turvajärjestelmä voidaan asentaa keskitetysti tiedon vastaanotto/välityspisteeseen. Yksittäisten tietokoneiden osalta, mukaan lukien myös matkapuhelimet ja PDA (Personal Digital Assistant) –laitteet, järjestelmä on mahdollista toteuttaa operaattorin tarjoamana palveluna tai uudenlaisena tietokoneena, joka sisältää keksinnön mukaisesti useamman järjestelmän (alijärjestelmät 1-3). Turvajärjestelmä ei välttämättä vaadi lisälaitteistoja toimiakseen, vaan se on monesti ohjelmallisesti toteutettavissa jo olemassa olevassa järjestelmässä sen verkkoelementtejä kuten palvelin tai reititin hyödyntäen, jotka verkkoelementit sisältävät muistin, esim. RAM –muistipiirin ja haihtumattoman muistin kuten kovalevyn, tiedon, esim. tietokoneohjelman, tallentamiseksi sekä suorittimen mainitun ohjelman määrittelemien toimintojen toteuttamiseksi.

Keksinnön toisen edullisen suoritusmuodon mukaan alijärjestelmä 2 jätetään turvajärjestelmän toteutuksesta pois, mikäli voidaan taata suojauskomennon saapuminen alijärjestelmään 3 ennen muuta, mahdollisesti virustartunnan saanutta, viestiliikennettä. Tällöin saavutetaan yhä korkea suojataso virushyökkäysten varalta ja järjestelmä on kokonaisrakenteeltaan edellistä suoritusmuotoa yksinkertaisempi mahdollistaen myös aikaisempaa alhaisemmat laitteistovaatimukset.

Keksinnön erään toisen edullisen suoritusmuodon mukaan muodostetaan turvajärjestelmä tiedon eristämiseksi kahden järjestelmän välillä. Tiedostot siirretään ulkoisesta järjestelmästä sisäiseen järjestelmään, esim. alijärjestelmään 3 eli käyttäjän järjestelmään, portaittain alijärjestelmien 1 ja 2 kautta. Tietojen eristämiseksi käyttäjän alijärjestelmän 3 ja ulkoisen järjestelmän välillä yhteys ulkoisen järjestelmän ja alijärjestelmän 1 välillä katkaistaan kun yhteys alijärjestelmien 1 ja 2 välillä on auki, ja yhteys alijärjestelmien 1 ja 2 välillä katkaistaan kun yhteys alijärjestelmien 2 ja 3 välillä on auki. Vastaavasti voidaan toimia myös siirrettäessä tietoa sisäisestä järjestelmästä ulkoiseen järjestelmään. Esitetyn alijärjestelmien välisen, portaittaisen viestiliikenteen avulla voidaan hankaloittaa luvatonta tunkeutumista käyttäjän järjestelmään.

Keksinnön edullisia suoritusmuotoja kuvataan epäitsenäisissä patenttivaatimuksissa.

Seuraavassa keksintöä selostetaan yksityiskohtaisemmin oheisiin piirustuksiin viittaamalla.

Kuvio 1 esittää keksinnön ensimmäisen edullisen suoritusmuodon mukaista turvajärjestelmää, joka on kytketty ulkoiseen järjestelmään reitittimen avulla, ja jonka alijärjestelmä 3 sisältää kolme käyttäjien tietokonetta sekä sähköpostipalvelimen,

kuviot 2A ja 2B esittävät keksinnön mukaisen turvajärjestelmän eri alijärjestelmiä ja niiden välisiä liitäntöjä,

kuvio 3 esittää vuokaaviota keksinnön mukaisessa turvajärjestelmässä suoritettavan virustentorjuntamenetelmän eräästä toteutusvaihtoehtoehdosta,

kuvio 4 esittää keksinnön toisen edullisen suoritusmuodon mukaista turvajärjestelmää, jossa alijärjestelmä 2 on jätetty turvajärjestelmän toteutuksesta pois,

kuvio 5 esittää keksinnön kolmannen edullisen suoritusmuodon mukaista turvajärjestelmää tietojen eristämiseksi ulkoisesta verkosta,

kuvio 6 esittää keksinnön mukaista laitetta ja siihen liitettyä muuta järjestelmää.

Kuviossa 1 esitetään pienyrityksen sisäinen tietoverkko, ns. lähiverkko, joka toimii samalla käyttäjän järjestelmänä ja keksinnön mukaisen turvajärjestelmän kolmantena alijärjestelmänä 3 sisältäen kolme mikrotietokonetta 104, 106, 108 ja sähköpostipalvelimen 102. Viestintä verkossa tapahtuu keskittimen (HUB) 112 lävitse. Yhteydet ulkoiseen järjestelmään 114, esim. maanlaajuiseen tietoverkkoon, on järjestetty kulkevaksi reitittimen 110 kautta. Palvelimen 102 ja reitittimen 110 toiminnal-

lisuudet voidaan haluttaessa toteuttaa myös samassa tietokoneessa. Turvajärjestelmän alijärjestelmät 1 ja 2 sijoittuvat tässä esimerkissä reitittimen 110 yhteyteen, mutta oleellisinta keksinnön kannalta on se, että mahdollisesti virustartunnan saaneet sähköpostit eivät pääse alijärjestelmään 3 tai ulkoiseen järjestelmään 114 ennen niiden tarkistamista sopivassa väliportaassa, joka voidaan tarvittaessa erottaa lähiverkosta. Täten turvajärjestelmä voidaan yleisessä tapauksessa sisällyttää esim. yhteen tai useampaan erilliseen tietokoneeseen ulkoisen verkon yhdyskäytävän ja sisäisen verkon väliin. Mikäli tämä ei kuitenkaan ole mahdollista, voidaan turvajärjestelmä toki toteuttaa kussakin lähiverkon tietokoneessa erikseen. Internetissä IP (Internet Protocol) siirtokerroksen tehtävänä on reitittää IP –data oikealle vastaanottajalle. Tavallisesti DNS (Domain Name Service) -palvelinten tietokannat sisältävät erityisiä MX (Mail eXchanger) -alkioita, jotka määrittelevät verkkotunnuksille omat postipalvelimensa, joihin kaikki kyseisiin tunnuksiin osoitettu posti välitetään. Postipalvelimet, esim. yleiset SMTP (Simple Mail Transfer Protocol) / POP (Post Office Protocol) -palvelimet, pyritään saamaan mahdollisimman toimintavarmoiksi ja niitä voi toisaalta toimia saman verkkoalueen sisällä useampiakin eri tavoin priorisoituina, jotta viestit tallentuisivat järjestelmään, vaikkei vastaanottajaa heti tavoitettaisikaan. DNS –palvelu voi kuviossa 1 esitetyssä tietoverkossa olla sijoitettuna esim. reitittimeen 110, joka ohjaa lähiverkkoon 3 saapuvan postiliikenteen automaattisesti palvelimelle 102. Lisätietoa viestiliikenteen reitityksestä DNS –järjestelmän osalta on löydettävissä mm. viitteestä [1]. Reitittimeen voidaan myös sisällyttää NAT (Network Address Translation) toiminnot, joiden avulla sisäisen tietoverkon koneet ovat sijoitettavissa eri(tyyppiseen) osoiteavaruuteen kuin mitä ulkoisessa verkossa käytetään.

Palvelin 102 ja tietokoneet 104, 106, 108 ovat kytkettynä Ethernet –tyyppiseen lähiverkkoon erillisen keskittimen 112 avulla. Muita mahdollisia verkkoratkaisuja ovat mm. Token Ring, FDDI (Fiber-Distributed Data Interface) ja ATM (Asynchronous Transfer Mode). Lähiverkossa eli turvajärjestelmän alijärjestelmässä 3 käytetty kaapelointi voi olla esim. pari- tai koaksiaalikaapelia. Toisaalta langattomiakin ratkaisuja kuten WLAN (Wireless LAN) on mahdollista hyödyntää esim. kannettavien tietokoneiden, matkapuhelimien tai PDA -laitteiden verkkoon liittämiseksi. Keskitin 112, joka sisältää useita portteja tietokoneiden kytkemiseksi, lähettää oletusarvoisesti yhdestä portista saamansa datan kaikkiin muihin portteihin. Täten aikaansaatu verkkotopologia on vain näennäisesti tähtimäinen, koska kyseessä on edelleen looginen väylä; väylään kytketyt laitteet havaitsevat halutessaan myös kaikkien muiden lähettämät viestit. Pääsymekanismi perustuu Ethernet –verkoissa kilpavaraukseen ja on nimeltään CSMA/CD (Carrier Sense Multiple Access / Collision Detect), jossa tietokone ensiksi kuuntelee, onko verkko vapaa ja vasta sen jäl-

keen aloittaa datan pakettimuotoisen lähettämisen. Useampi kone voi aloittaa lähettämisen yhtä aikaa, joten myös lähettäjän on kuunneltava väylää lähettämisen aikana mahdollisten datansiirtotörmäysten varalta. Havaitessaan törmäyksiä lähettäjä vaikenee satunnaiseksi ajanjaksoksi ennen uusintalähetystä.

Alijärjestelmän 3 sisällä data ohjataan tietokoneesta tai laitteesta toiseen ns. MAC- eli laiteosoitteiden (Medium Access Control) ja ulkoiseen verkkoon/verkosta IP –osoitteiden avulla. Jokaisella verkkoon liitetyllä laitteella on siten oma MAC- ja IP –osoitteensa. ARP –protokolla (Address Resolution Protocol) mahdollistaa IP-osoitetta vastaavan MAC-osoitteen selvittämisen lähiverkossa. Osoitekysely lähetetään verkkoon ilman määrättyä vastaanottajaa, mutta reititin 110 ei välitä kyselyä lähiverkosta eli tässä tapauksessa alijärjestelmästä 3 ulos. Laite, joka tunnistaa kyseessä olevan IP -osoitteen, vastaa suoraan kysyjälle. Opittuaan haetun IP-MAC -vastaavuuden kysyjä merkitsee sen ARP -tauluunsa ja pystyy tulevaisuudessa lähettämään datakehyksen suoraan vastaanottajalle ilman kyselyjä. Lähetettäessä dataa alijärjestelmästä 3 ulos tulee se aluksi siirtää reitittimelle 110, joka hoitaa datansiirron ulkomaailman kanssa. Jos lähettäjä itse havaitsee datan suuntautuvan lähiverkon ulkopuolelle, se voi ohjata viestiliikenteen suoraan reitittimelle 110, jonka lähiverkko-osoite on lähettäjän tiedossa. Muussa tapauksessa laite yleislähettää ARP-sanoman, jossa kysytään paketin vastaanottajan IP-osoitetta vastaavaa lähiverkko-osoitetta. Reititin 110 havaitsee paketin vastaanottajan sijaitsevan alijärjestelmän 3 ulkopuolella ja vastaa kyselyyn omalla lähiverkko-osoitteellaan. Tämän jälkeen lähettäjä välittää viestin reitittimelle 110. Viestien reitittäminen perustuu lähiverkon ulkopuolella, esim. alueverkossa, tavallisesti jonkin sisäisen reititysprotokollan kuten RIP (Routing Information Protocol) ja OSPF (Open Shortest Path First) hyödyntämiseen. Autonomisten alueiden, esim. eri maiden verkko-operaattorien tai yritysten, välillä käytetään ns. ulkoisia reititysprotokollia, esim. BGP:tä (Border Gateway Protocol), koska reittiä ei tällöin valita pelkästään tehokkuuskriteerein, vaan valintaan vaikuttavat muutkin seikat, esim. poliittiset, talouteen tai turvallisuuteen vaikuttavat tekijät, jotka rajoittavat kulloinkin hyödynnettävien reittien valintaa. Mainitut rajoitukset ja reittimäärittelyt syötetään yleensä käsin reitittimiin. Lisätietoa tietoliikenneverkoista erityisesti järjestelmätasolla on saatavissa viiteteoksesta [2].

Kuviossa 2A esitetään viestin välittäminen ulkoisesta järjestelmästä 114 alijärjestelmään 3 turvajärjestelmän eri komponenttien kannalta. Reitittimen 110 yhteyteen sijoitettu, mutta edullisesti silti toiminnallisuudeltaan erillinen, alijärjestelmä 1 vastaanottaa kaiken välitettävän viestiliikenteen ulkoisen verkon ja alijärjestelmän 3 välillä. Alijärjestelmän 1 postikirjassa, joka voidaan toteuttaa esim. muistiin tallennettavana taulukkona, on kutakin alijärjestelmän 3 laitteen tunnistetta, esim. verkko-

tai laiteosoitetta, vastaava tunniste, joka sijaitsee alijärjestelmässä 2. Kun alijärjestelmä 1 vastaanottaa uuden viestin 202, se tallennetaan väliaikaisesti esim. RAM (Random Access Memory) –muistiin, eikä viestiä 202 käsitellä, avata tai millään tavoin muuteta ennen varsinaista vaihetta virusten aktivoimiseksi. Alijärjestelmä 1 sisältää oletusarvoisesti alijärjestelmän 3 kanssa yhteensopivan tietokonelaitteiston, tätä nykyä tyypillisesti esim. MSDOS (Microsoft Disk Operating System) / Windows –käyttöjärjestelmällä varustetun mikrotietokoneen. Vaikkakin reitittimessä 110 itsessäänkin saattaa olla muistikapasiteettia ja sen suorittimessa laskentatehoa esitetyn virustentorjuntamenetelmän suorittamiseksi koko laajuudessaan, myös erillistä, esim. reitittimen ja keskittimen väliin sijoitettavaa, tietokonelaitteistoa voidaan hyödyntää turvajärjestelmän toteuttamisessa. Tällöin ei mahdollinen virusaktivoituminen vaikuta välttämättä yhtä tuhoisasti reitittimen toimintaan ja sen sisältämiin viesteihin kuin täysin yhdistetyssä reititin/turvajärjestelmä –ratkaisussa. Myös alijärjestelmä 2 voidaan haluttaessa erottaa alijärjestelmästä 1 omaan laitteistoonsa. Seuraavaksi alijärjestelmässä 1 tehdään haku viestiin 202 mahdollisesti kiinnittyneiden virusten havaitsemiseksi. Mikäli virus havaitaan, suoritetaan hälytys, ts. lähetetään suojauskäsky 204 alijärjestelmille 2 ja 3. Vaihtoehtoisesti, jos havaittu virus on tunnettua tyyppiä ja turvajärjestelmän toimesta varmuudella poistettavissa saastuneesta viestistä, voi turvajärjestelmä jatkaa normaalia toimintaansa kuitenkin tallentaen tiedon virushavainnosta ja tehdyistä korjaavista toimenpiteistä esim. erityiseen lokitiedostoon. Puhdas viesti välitetään alijärjestelmän 2 kautta vastaanottajalle alijärjestelmään 3.

Alijärjestelmiin 1 ja 2 voidaan liittää järjestelmä X, esim. alijärjestelmä 210 eli ns. "kaatopaikka", jonne suojauskäskyn saapuessa tallennetaan hälytyksen aiheuttanut viesti sekä esim. muut alijärjestelmässä 2 sillä hetkellä olevat viestit ja tiedostot jatkotutkimuksia varten. Tällöin, mikäli turvajärjestelmän turvalliselle toiminnalle asetetut ehdot yhä täyttyvät, alijärjestelmät 1 ja 2 voivat lähes viivästyksettä jatkaa normaalia toimintaansa, kun liitetty järjestelmä 210 huolehtii varsinaisesta virusanalysoinnista. Yhdeksi turvallisen toiminnan ehdoksi voidaan asettaa esim. alijärjestelmien 1 ja 2 uudelleenkäynnistäminen ja/tai niiden käyttömuistin tyhjennys.

Kuviossa 2B esitetään vastaavasti viestin välittäminen lähiverkosta eli turvajärjestelmän alijärjestelmästä 3 ulkoiseen järjestelmään 114. Mikäli alijärjestelmästä 3 lähetetystä viestistä 206 löydetään virus, lähetetään suojauskäsky 208 välittömästi alijärjestelmille 1 ja 2. Kuvioiden 2A ja 2B sisältämät vastaanotto- ja lähetyssuunnan alijärjestelmät 1 ja 2 sisältävät logiikaltaan samanlaiset toiminnot ja ne voidaan haluttaessa sijoittaa fyysisesti joko yhteisiin tai erillisiin laitteistoihinsa. Mikäli toteutettu ratkaisu nojaa ainakin osittain yhteiseen laitteistoon, tulee suojauskäskyt edul-

lisesti välittää molempien tiedonsiirtosuuntien alijärjestelmille 2 ja 3 siten, että virushavainnon jälkeen viestiyhteydet myös katkeavat molempiin suuntiin. Tällöin varmistutaan siitä, että virukset eivät pääse lenkittymään takaisin tulosuuntaansa ja siten saastuttamaan mahdollisesti vielä uusia tietokoneita.

Kuviossa 3 esitetään vuokaavio keksinnön mukaisen turvajärjestelmän alijärjestelmässä 1 suoritettavan virustentorjuntamenetelmän eräästä edullisesta toteutusvaihtoehtoehdosta. Alijärjestelmän 1 toimintaa tarkkaillaan 302 resurssien, esim. laskentatehon, salliessa jatkuvasti, eikä vain silloin kuin viesti vastaanotetaan 304 ulkoisesta järjestelmästä 114 tai alijärjestelmästä 3. Joskus saattaa olla välttämätöntä asettaa virushaun maksimikestolle raja-arvo, jota ei saada ylittää. Raja-arvon mahdollistamalla maksimaalisella hakuajalla, joka määrittelee osaltaan myös esitetyn virustentorjuntamenetelmän viestinvälitykseen tuoman, ehkä järjestelmän spesifikaatiossakin mainitun, maksimiviiveen, tulee voida keskimäärin luotettavasti havaita virustartunnan saaneet viestit, mutta poikkeustapauksissa saattaa esim. aktivoitumistavaltaan tai muulla tavoin tuntemattoman viruksen saastuttamia viestejä päästä turvajärjestelmän seulasta lävitse. Tällöinkin on toki tapauskohtaisesti mahdollista säästyä lisävahingoilta tai pienentää niitä, jos virus yleensä edes jossakin vaiheessa havaitaan, vaikka se olisikin jo päässyt käyttäjän järjestelmään. Turvajärjestelmän tarkkailemista käsitellään myöhemmin yksityiskohtaisemmin virusten aktivointiyritysten kuvauksen yhteydessä. Mikäli tarkkailu paljastaa viruksen 303, suoritetaan hälytys ja lähetetään suojauskäsky 316.

Virushaun ensimmäisessä vaiheessa välitettävästä viestistä etsitään viruksia perinteisten virustentorjuntaohjelmien keinoin 306 ennalta tunnettujen virusten löytämiseksi. Tähän tarkoitukseen voidaan käyttää esim. tietokantaa virusten sormenjäljistä. Mikäli ensimmäinen vaihe paljastaa virustartunnan 308, alijärjestelmä 1 lähettää suojauskäskyn 316 alijärjestelmille 2 ja 3. Muussa tapauksessa etsintää jatketaan toiseen vaiheeseen, jossa yritetään saada tuntematon virus aktivoitumaan 310 ja siten paljastamaan itsensä. Turvajärjestelmä käy lävitse esim. kaikki ne aktivointitavat, joilla virusten tiedetään aktivoituvan ja mahdollisesti yhdistelee niitä joko samanaikaisesti tai peräkkäin tapahtuviksi. Uusia aktivoitumistapoja voidaan toisaalta lisätä järjestelmään sitä mukaa, kun niitä tulee ilmi. Turvajärjestelmän havaitsemat uudet aktivoitumistavat voidaan myös ohjelmoida tallentuvan automaattisesti sen virustietokantaan. Turvajärjestelmää tarkkaillaan epätavallisten ja siten mahdollisesti virusten suorittamien tai niiden välillisesti aikaansaamien toimintojen havaitsemiseksi 311. Viruksen aktivoituminen turvajärjestelmässä on lähtökohtaisesti suotuisampaa kuin aktivoituminen käyttäjän järjestelmässä, koska turvajärjestelmä voidaan virusaktivoitumisen jälkeen eristää nopeasti ja toisaalta se ei sisällä rele-

vanttia tietoa kuin korkeintaan muutaman vielä turvajärjestelmässä sijaitsevan välittämättömän viestin osalta. Useimmiten tietoliikenneverkoissa lähetetyt viestit tallentuvat myös lähettäjän postilaatikkoon, jolloin virusaktivoitumisen seurauksena välitysvaiheessa tuhoutuneidenkin viestien uusintalähetys on yleensä mahdollista ilman suuria ongelmia. Virusten aktivoitumiset voidaan jakaa niiden etsinnän kannalta kahteen pääryhmään: tunnettuihin ja tuntemattomiin aktivoitumistapoihin. Jos viruksen aktivoituminen havaitaan 312, suoritetaan hälytys ja lähetetään suojauskäsky 316, muussa tapauksessa viesti välitetään normaalisti eteenpäin 314 alijärjestelmän 2 kautta.

Tunnettuihin virusten aktivoitumistapoihin sisältyvät aikaan sidotut aktivoitumiset. Aikaa hyödyntävä virus saattaa aktivoitua ollessaan esim. kolmannen kerran järjestelmässä, jonka päiväys on 10.9.2002. Tämäntyyppisen viruksen havaitsemiseksi voidaan mm. järjestelmän aikatietoa, ns. kelloa, juoksuttaa eteenpäin ja taaksepäin, jolloin juoksutus on mahdollisesti suoritettava useampaan kertaan riittävän aktivointipäivämäärän ohituskertojen lukumäärän takaamiseksi. Turvajärjestelmän suorittamien juoksutuskertojen lukumäärä tulee olla suurehko, vaihtuva tai ainakin jollakin tapaa käyttäjän määriteltävissä, jotta tietyt aikasidonnaiset virukset eivät pääsisi säännöllisesti etsinnöistä lävitse jo lähtökohtaisesti liian pienen juoksutusmäärän takia. Toisaalta esim. muistinhallintaan sidottuja aktivoitumisia voidaan seuloa samaan tapaan moninkertaisten muistintäyttösilmukoiden avulla, joissa muistipaikkoja käydään toistuvasti läpi esim. kirjoittamalla niihin näennäisdataa. Osa viruksista aktivoituu, kun massamuistin kuten kovalevyn tiedostoja käsitellään. Tämäntyyppisten virusten aktivoitumista voidaan edesauttaa turvajärjestelmän suorittamalla automaattisella tiedostojen käsittelyllä, esim. näennäistiedostoja lukemalla tai niihin kirjoittamalla sekä näennäistiedostoja generoimalla ja poistamalla. Myös tiedostojenhallintaan liittyvien funktioiden kutsuminen eli pelkkä tiedostokäsittelyn osittainen simulointi, saattaa riittää virusten aktivointiin. Edellä mainittujen tapojen lisäksi käytetään toisaalta muitakin tiedossa olevia virusten aktivointikeinoja ottaen huomioon kunkin aktivoitumistavan erityispiirteet.

On mahdollista, että viruksen aktivoituminen perustuu useamman erillisen ehdon yhtäaikaiseen tai peräkkäiseen täyttymiseen. Viruksen aktivoitumisehdot saattavat toisaalta vaihtua viruksen edetessä laitteistosta toiseen. Tällöin voidaan monipuolisilla ja moninkertaisilla aktivointiyrityksillä silti pienentää viruksen todennäköisyyttä läpäistä turvajärjestelmä. Turvajärjestelmä voi joko käyttäjän ohjelmoiman, siihen esim. julkaisuvaiheessa esiohjelmoidun tai ainakin osittain satunnaisuuteen pohjautuvan ohjauslogiikan perusteella päättää käytetyistä aktivointikeinoista, niiden toistojen määrästä ja hyödynnettävistä aktivointikeinojen kombinaatioista. Ku-

vion 3 menetelmässä vaiheita 310 ja 311 voidaan siten toistaa mainitun logiikan mukaan ennen viestin lopullista virusvapaaksi toteamista ja välittämistä eteenpäin. Jos erillisiä turvajärjestelmiä sijoitetaan viestiketjussa useampaan kohtaan, järjestelmän kokonaisturvataso nousee moninkertaisten, riippumattomien tarkistusten jälkeen varsin korkealle tasolle.

Täysin ennalta tuntemattomien virusten ja niiden aktivoitumistapojen löytämiseksi voidaan toisaalta yrittää joko ennakoida mahdollisia uusia aktivoitumistapoja tai käyttää jotakin erityistä menetelmää virustartunnan tai -aktivoitumisen aiheuttaman johdannaisvaikutuksen havaitsemiseksi. Eräs menetelmä, jonka avulla havaitaan poikkeavuuksia välitettävissä viesteissä, perustuu viestien moninkertaiseen lähettämiseen. Kyseisessä menetelmässä sähköpostin lähettäjä lähettää ainakin kaksi viestiä A ja B, joka viesti B on joko viestin A identtinen kopio tai vähintäänkin tarkka kuvaus viestin A koostumuksesta. Viestien A ja B vertailu voidaan suorittaa jo lähetyspäässä, lähetyssuunnan turvajärjestelmän alijärjestelmässä 1. Alijärjestelmä 1 osaa vertailla juuri oikeita viestejä viesteinä A ja B tunnettua tunnistamistekniikkaa hyväksikäyttäen. Jos esim. viesteille muutoinkin annetaan yksilöllinen ID (IDentifier) –tunniste, voidaan siihen vielä lisätä kirjaimet A ja B kuvaamaan saman viestin eri kopioita. Tunnisteena on mahdollista käyttää lähes mitä tahansa viestin jollakin tavalla yleensä yksilöllistä osaa otsikkokentästä ja sen sisällöstä hyötykuormaan tai sen osaan. Mikäli vertailussa ei havaita mitään poikkeavaa, ts. viestit ovat joko tunnisteita ja mahdollisesti tarkkaa lähetysaikaa lukuun ottamatta identtiset tai viestin B kuvaus viestistä A pitää täsmälleen paikkansa, lähettää lähetyspään lähetyssuunnan turvajärjestelmän alijärjestelmä 1 viestin A eteenpäin ja joko arkistoi tai hävittää viestin B. Jos vertailussa havaitaan poikkeavuuksia, aiheuttavat ne virushälytyksen, koska poikkeavuus saattaa johtua viruksen kiinnittymisestä jompaankumpaan viestiin. Yksinkertainen tekniikka saastuneen viestin erottamiseksi vahingoittumattomasta perustuu viestin uusintalähetykseen, jossa alijärjestelmä 1 pyytää lähettäjää lähettämään viestin vielä kertaalleen, ja viestin saavuttua vertailee sitä edellisiin viesteihin. Käytännössä tämä voidaan toteuttaa niin, että lähetyspään lähetyssuunnan turvajärjestelmä ilmoittaa lähetyspään vastaanottosuunnan turvajärjestelmälle, jotka ovat siten tiedonsiirtoyhteydessä myös keskenään, esim. viestin avulla, että lähettäjältä toivotaan viestin uusintalähetystä. Tämän jälkeen vastaanottosuunnan turvajärjestelmä välittää pyynnön lähettäjälle, joka lähettää viestistä uuden kopion. Vaihtoehtoisesti lähetyssuunnan turvajärjestelmä voi sisältää oman paluukanavan alijärjestelmään 3 esim. kuittausviestien tai uudelleenlähetyspyyntöjen välittämiseksi. Mikäli turvajärjestelmä on järjestetty kuittaamaan lähettäjälle kaikki virheettömästi vastaanotetut välitettäväksi tarkoitetut viestit, voidaan kuittaus jättää tarkoituksellisesti tekemättä, jolloin lähettäjä automaattisesti lähettää viestistä toisen ko-

pion, joka kuitataan nyt normaaliin tapaan. Viestin kopioiden vertailussa voidaan esim. tiedostokoon kasvamisesta päätellä, mihin viestiin tai viesteihin virus on kiinnittynyt.

Edellä esitetty viestien moninkertaiseen lähettämiseen pohjautuva menetelmä on sovellettavissa vastaavasti myös vastaanottopäässä, jolloin ulkoisesta järjestelmästä saapuu vastaanottosuunnan turvajärjestelmän alijärjestelmään 1 ainakin kaksi tunnisteidensa avulla toisiinsa assosioitavissa olevaa viestiä, joita vertaillaan poikkeavuuksien havaitsemiseksi. Mikäli ulkoinen järjestelmä ei automaattisesti lähetä tai sitä ohjelmoida lähettämään viestistä useampaa kopiota, turvajärjestelmä voi halutessaan pyytää ulkoiselta järjestelmältä jo vastaanotetun viestin uudelleenlähetystä esim. postinvälitysprotokolliin valmiiksi ohjelmoituja perustoimintoja, joita ovat mm. viestin uudelleenlähetyspyyntö ja kuittaus vastaanotetusta viestistä, hyödyntämällä ja siten saada useamman kopion viestistä tutkittavaksi. Uudelleenlähetyspyyntö voidaan toimittaa joko viestin alkuperäiselle lähettäjälle tai vaihtoehtoisesti esim. ulkoisen järjestelmän postipalvelimelle, joka välittää pyynnön eteenpäin lähettäjälle tai toimittaa mahdollisesti muistiinsa tallennetun kopion viestistä turvajärjestelmälle. Viimeksi mainitussa vaihtoehdossa viruksen havaitseminen voi tosin olla lähtökohtaisesti vaikeampaa, koska viestinvälitysketjusta jää kopion osalta alkuperäisen lähettäjän suorittama osuus kokonaan pois. Uudelleenlähetyspyyntö on mahdollista ehdollistaa koskevaksi vain osaa kaikista viesteistä. Esim. vain liitetiedostoja sisältävät viestit tutkitaan vertailun avulla, koska juuri liitetiedostot toimivat useimmiten viruksenkantajina.

Edellä kuvatussa järjestelyssä viestit luodaan samassa järjestelmässä (lähettäjä joko alijärjestelmässä 3 tai ulkoisessa järjestelmässä), joten teoriassa on toki mahdollista, että virus sisältyy kaikkiin viesteihin ja ilmenee niissä samalla tavoin. Tällöin viestien keskinäinen vertailu ei tuota tulosta, jos esim. saastunut liitetiedosto on niissä kaikissa mukana. Tämän riskin eliminoimiseksi voidaan haluttaessa rakentaa turvajärjestelmä siten, että lähettäjän eli lähetyspään turvajärjestelmän alijärjestelmän 3 ohjausyksikköjen (näppäimistö, hiiri jne.) rinnalle kytketään toinen järjestelmä, esim. lähetyssuunnan turvajärjestelmän alijärjestelmä 1, joka sisältää alijärjestelmän 3 ohjelmat ja tiedot niin, että viesti B generoituu ja tallentuu rinnakkaiseen järjestelmään samalla tavoin kuin viesti generoituu ja tallentuu tai ainakin haluttaessa tallentuisi alijärjestelmissä 1-3. Vaihtoehtona tarkistusviestin B (A) lähettämiselle alijärjestelmään 1 onkin nyt, että lähetetään ainoastaan viesti A (B) ja ainakin yksi tarkistusviesti B (A) tallennetaan lähettävään ja/tai rinnakkaiseen järjestelmään ja vertailun suorittava järjestelmä, alijärjestelmä 1, tekee vertailun mainitussa lähettäväs-sä/rinnakkaisessa järjestelmässä. Alijärjestelmä 1 voidaan esim. ohjelmoida ana-

lysoimaan viesti A sen ominaispiirteiden selvittämiseksi ja kytkeytymään sen jälkeen rinnakkaiseen järjestelmään mainittujen ominaispiirteiden vertailemiseksi kyseiseen rinnakkaiseen järjestelmään tallennetun viestin B ominaispiirteiden kanssa. Mikäli alijärjestelmä 1 on itse myös mainittu rinnakkainen järjestelmä eli se tallentaa viestin B jo sen teko- tai viimeistään lähetysvaiheessa ja toisaalta vastaanottaa viestin A normaalisti, on vertailu varsin helppoa erilliseen rinnakkaiseen järjestelmään kytkeytymisen ollessa näin tarpeetonta.

Toisaalta rinnakkainen järjestelmä voidaan kytkeä lähetyspäässä lähetyssuunnan turvajärjestelmään tai vaihtoehtoisesti johonkin muuhun viestinvälitykseen soveltuvaan verkkoelementtiin siten, että kyseinen rinnakkainen järjestelmä välittää viestejä eteenpäin joko ohi tai läpi lähetyspään turvajärjestelmän. Tällöin jäljempänä viestiketjussa, esim. vastaanottopäässä, vastaanottosuunnan turvajärjestelmä vertailee viestejä kuten aikaisemmin on jo kuvattu, erona aiemmin esitettyyn viestien vertailuratkaisuun lähinnä se, että toinen viesteistä onkin peräisin lähettäjän järjestelmään kytketystä rinnakkaisesta järjestelmästä eikä itse lähettäjältä. Vastaanottopään turvajärjestelmä voi tarvittaessa pyytää viestin uusintalähetystä lähetyspään turvajärjestelmältä tai vaihtoehtoisesti lähettäjältä/rinnakkaiselta järjestelmältä joko suoraan tai välillisesti turvajärjestelmän kautta.

Turvajärjestelmän tarkkailussa keskitytään mm. seuraaviin seikkoihin virusten todentamiseksi:

Alijärjestelmässä 1 tapahtuu jokin muutos ennen kuin alijärjestelmä 1 on viruksen paljastamiseksi itse tehnyt muutoksia aiheuttavia toimenpiteitä,

alijärjestelmässä 1 tapahtuu muutos, jossa ei ole kysymys alijärjestelmän viruksen paljastamiseksi tekemästä toimenpiteestä,

viesti lähtee alijärjestelmään 2 tai muuhun järjestelmään ilman alijärjestelmän 1 käskyä,

viesti lähtee alijärjestelmään 2 tai muuhun järjestelmään, mutta väärään osoitteeseen tai järjestelmään X, jos sellainen on kytketty, mutta johon ei ole lähtökohtaisesti suunnattu viestiliikennettä,

viesti ei lähde alijärjestelmään 2 tai muuhun järjestelmään, vaikka alijärjestelmä 1 on sen sinne lähettänyt,

järjestelmän tarkkailuohjelmisto havaitsee aktivoituneen viruksen jollakin muulla perusteella.

Alijärjestelmän 1 välittäessä hälytyksen seurauksena suojauskäskyn 316 alijärjestelmille 2 ja 3 alijärjestelmät 1-3 katkaisevat tiedonsiirtoyhteytensä esim. siten, että ne eivät voi enää vastaanottaa tai lähettää viestejä. Oleellista suojauskäskyn aiheuttamissa toimenpiteissä on, että viestiliikenne alijärjestelmien 1 ja 2 sekä käyttäjän järjestelmän välillä ei enää kulje, kunnes virushälytyksen syy on selvitetty ja mahdollisesti saastuneet tiedostot puhdistettu. Eräs toimintamalliltaan yksinkertainen vaihtoehto turvajärjestelmän puhdistamiseksi on alijärjestelmien 1 ja 2 uudelleenasentaminen, haluttaessa kuitenkin vasta sen jälkeen, kun halutut tiedot on siirretty joko automaattisesti tai käyttäjän antaman komennon jälkeen alijärjestelmään 210 myöhempää analysointia varten. Mahdollinen virustentorjuntajärjestelmän virushälytyksen laukeamisesta ja siihen liittyvistä suojaus/analysointitoimenpiteistä johtuva palvelutauko koskien ulkoisen verkon ja suojattavan järjestelmän välistä viestiliikennettä voidaan minimoida varajärjestelmän, esim. rinnakkaisen turvajärjestelmän, käyttöönotolla. Mikäli virus saadaan alijärjestelmässä 210 analysoitua, voidaan siitä myöhemmin lähettää "sormenjäljet" muille tunnetuille turvajärjestelmille ja turvajärjestelmän kehittäjän palvelimelle esim. lisättäväksi asiakkaille säännöllisesti toimitettavaan virustietokantaan, jotta kyseinen virus saadaan myöhemmin tunnistettua jo virushaun ensimmäisessä vaiheessa 306.

Suojauskäsky lähetetään edullisesti erillistä ja suojattua yhteyttä hyväksikäyttäen alijärjestelmille 2 ja 3, vaikkakin myös normaalin viestinvälityksen kanssa yhteinen datalinkki on mahdollinen. Suojauskäskyn välittämisen kannalta on tärkeää, että käsky saadaan mahdollisimman nopeasti ja luotettavasti toimitettua vastaanottajalle ja suojauskäskyn tuleekin saavuttaa vastaanottaja eli alijärjestelmä 2 tai 3 ennen kuin virus ehtii tehdä vahinkoa kyseisissä järjestelmissä tai levitä eteenpäin. Esim. saastuneen viestin saapuessa ulkoisesta järjestelmästä 114 reitittimelle 110 alijärjestelmästä 1 lähtevän suojauskäskyn on saavutettava alijärjestelmä 3 ennen virusta ja yhteys alijärjestelmien 2 ja 3 välillä tulee voida katkaista, jotta saastunut viesti ei välittyisi lainkaan alijärjestelmään 3. Yhteyksien katkaiseminen on mahdollista suorittaa esim. ohjelmallisesti sulkemalla tiedonsiirtopalvelut kyseisissä alijärjestelmissä. Jos käyttäjän järjestelmä, alijärjestelmä 3, hyödyntää esim. perinteisiä 10Mbit/s Ethernet -linkkejä, mutta keskittimessä 112 on tarvittava logiikka hoitamaan 10<->100Mbit/s nopeuskonversiota sekä eri linkkien välistä priorisointia, voidaan reitittimen 110 yhteyteen sijoitetun turvajärjestelmän alijärjestelmä 1 liittää suoraan 100 Mbit/s linkin kautta keskittimeen 112, joka on ohjelmoitu antamaan korkein prioriteetti 100 Mbit/s –linkin kautta kulkevalle datalle. Turvajärjestelmän toteuttavassa laitteistossa määritetään suojauskäskylle tietty muoto tai ainakin tietty tunniste, jonka avulla vastaanottajat voivat sen identifioida. Myöskin mikäli yhteys suojauskäskyn lähettäjältä sen vastaanottajalle on erillinen, voidaan ajatella lähes minkä tahan-

sa sitä kautta lähetetyn datan olevan riittävä peruste yhteyksien katkaisemiseksi. Tällöin viruksen päästyä käsiksi turvajärjestelmään ja lähettäessä omia viruksin varustettuja viestejä erillistä yhteyttä käyttäen, myös ne laukaisevat hälytyksen. Turvajärjestelmän toteuttavalle ohjelmistolle ja prosesseille, koskien kaikkia alijärjestelmiä 1-3, tulee määritellä korkeat suorituspriorititeetit, jotta suojauskäskyjen lähettäminen ja vastaanottaminen suoritetaan viipymättä, riippumatta siitä, välitetäänkö suojauskäsky erillistä yhteyttä pitkin vai ei. Alijärjestelmä 2 voidaan asettaa tarkoituksella viivästyttämään viestien välitystä esim. käyttäjän säädeltävissä olevan parametrin kautta, jotta mahdollisen suojauskäskyn saapuessa ei saastuneita viestejä varmasti ole vielä ehditty lähettää eteenpäin. Toisaalta keskitin 112 tai muu vastaava alijärjestelmän 3 solmuelementti on mahdollista ohjelmoida ymmärtämään suojauskäskyt ja sulkemaan kauttaan kulkevat tietoliikenneyhteydet. Tällöin ei alijärjestelmän 3 jokaiselle elementille tarvitse erikseen muodostaa erillistä yhteyttä alijärjestelmään 1 tai ohjelmoida tukea suojauskäskyn tulkitsemiseksi.

Keksinnön toisessa edullisessa suoritusmuodossa, katso kuvio 4, alijärjestelmä 2 jätetään turvajärjestelmän toteutuksesta pois, mikäli suojauskäsky 402 tavoittaa vastaanottajansa nopeammin kuin mitä saastuneen viestin lähettämiseen ja vastaanottamiseen kuluu aikaa. Alijärjestelmä 210 voidaan yhä säilyttää virusten analysoimiseksi. Suojauskäskyn nopea siirtäminen on toteutettavissa esim. nopean erillisen datayhteyden avulla. Myös turvajärjestelmän ohjelmiston suojauskäskyjen käsittelyyn liittyvien prosessien korkea prioriteetti ja muun viestinvälityksen hidastaminen maksimaalista alhaisemmalle tasolle parantavat virusten havaitsemismahdollisuuksia ennen niiden välittämistä eteenpäin. Toisaalta mainittu hidastaminen voidaan kytkeä itse virushavaintoon esim. niin, että alijärjestelmän 1 havaitessa viruksen se hidastaa omaa viestinvälitystään määritetyllä tavalla ja alijärjestelmät 2 ja 3 toimivat vastaavasti suojauskäskyn vastaanotettuaan. Tällöin saavutetaan yhä korkea suojataso virushyökkäysten varalta järjestelmän säilyessä rakenteeltaan yksinkertaisena mahdollistaen myös edellistä suoritusmuotoa alhaisemmat laitteistovaatimukset.

Kuvio 5 esittää keksinnön erästä toista edullista suoritusmuotoa, jossa edellä esitetty keksinnön ensimmäisen edullisen suoritusmuodon mukainen turvajärjestelmä eristää käyttäjän järjestelmän eli alijärjestelmän 3 ulkoisesta järjestelmästä 114 luvattomien tunkeutumisyritysten hankaloittamiseksi. Tiedot, esim. tiedostot ja viestit, siirretään ulkoisesta järjestelmästä 114 alijärjestelmään 3 alijärjestelmien 1 ja 2 kautta. Kuvion esimerkissä alijärjestelmä 1, jolla ei ole samanaikaisia yhteyksiä ulkoiseen järjestelmään ja alijärjestelmään 2, on saanut viestin ulkoisesta järjestelmästä. Seuraavaksi yhteys ulkoisen järjestelmän 114 ja alijärjestelmän 1 välillä katkaistaan ennen yhteyden muodostamista alijärjestelmien 1 ja 2 välille ja viestin välittä-

mistä alijärjestelmään 2, katso kuvion vaihe A. Tämän jälkeen yhteys alijärjestelmien 1 ja 2 välillä katkaistaan ennen yhteyden muodostamista alijärjestelmien 2 ja 3 välille ja viestin välittämistä vastaanottajalle alijärjestelmään 3, katso kuvion vaihe B. Nyt myös yhteys ulkoisen järjestelmän 114 ja alijärjestelmän 1 välillä voidaan jälleen avata, vrt. katkoviiva kuviossa. Täten suoraa reaaliaikaista yhteyttä ulkoisen järjestelmän 114 ja alijärjestelmän 3 välillä ei esiinny ja alijärjestelmä 3 on eristetty. Yhteyksien katkaiseminen voidaan toteuttaa esim. ohjelmallisesti sulkemalla tiedonsiirtopalvelut alijärjestelmissä 1 ja 2. Alijärjestelmään 3 kohdistuvat hyökkäysyritykset voivat silti perustua mm. viesteissä lähetettyihin vihamielisiin ohjelmiin (vrt. troijalaiset hevoset), jotka suorittavat piilotoiminteita kuten tiedonkeruuta alijärjestelmässä 3 tai pyrkivät sotkemaan sen toimintaa. Tämäntyyppiset ohjelmat ovat kuitenkin havaittavissa alijärjestelmän 1 virustenhaku- ja aktivointimenetelmillä ennen niiden pääsyä alijärjestelmään 3. Vastaavanlainen menettely voidaan haluttaessa suorittaa myös siirrettäessä tietoa alijärjestelmästä 3 ulkoiseen järjestelmään 114. Kummassakin tiedonsiirtosuunnassa on toki muitakin portaittaisen tiedonsiirron takaavia vaihtoehtoja alijärjestelmien ja ulkoisen verkon välisten yhteyksien katkaisemiseksi ja muodostamiseksi, joissa reaaliaikaista yhteyttä ulkoisen järjestelmän ja alijärjestelmän 3 välillä ei missään vaiheessa pääse syntymään. Jos hyödynnetyt yhteydet ovat kaksisuuntaisia, voidaan vastaanottosuunnan alijärjestelmä 1 ja lähetyssuunnan alijärjestelmä 2 sekä toisaalta vastaanottosuunnan alijärjestelmä 2 ja lähetyssuunnan alijärjestelmä 1 sijoittaa edullisesti toistensa yhteyteen.

Keksinnön eräässä toisessa edullisessa suoritusmuodossa, katso kuvio 6, kytketään verkkoelementtiin kuten käyttäjän tietokoneeseen 602, reitittimeen, kytkimeen, palvelimeen 604 tai keskittimeen, laite 606 virusten aktivoimiseksi ja havaitsemiseksi. Kytkentä 608 on toteutettavissa esim. Ethernet –tyyppisen liitännän avulla perinteisesti parikaapelia hyödyntäen tai langattomasti WLAN –yhteyden lävitse. Aikaisemmista suoritusmuodoista poiketen laite 606 ei tässä tapauksessa välitä kauttansa viestejä, vaan sille siirretään ainakin osa verkkoelementin 602, 604 lähettämistä, lähetettäväksi tarkoitetuista tai vastaanottamista viesteistä tarkistettavaksi. Mikäli kaikkia viestejä ei säännöllisesti lähetetä mainitulle laitteelle 606 tai vaihtoehtoisesti laite 606 niitä itse verkkoelementiltä 602, 604 nouda, voidaan ohjelmoida ainakin esim. haluttu prosenttiosuus kaikista viesteistä välitettäväksi laitteelle 606 virushakua varten, ja tähän osuuteen sisältyvät viestit on mahdollista valita erityyppisten kriteerien perusteella. Eräänä kriteerinä voikin olla, että liitetiedostoja sisältävät viestit tarkistetaan aina. Laite 606, joka on esim. tietokone, sisältää oleellisesti samat ohjelmistot kuin aikaisemmin esitetyn turvajärjestelmän alijärjestelmä 1, minkä lisäksi siihen voidaan tarpeen mukaan sisällyttää alijärjestelmän 2 piirteitä joko samaan tai ainakin osittain eriytettyyn alilaitteistoonsa. Esim. verkkoelementiltä 602,

604 tarkastettavaksi saatujen viestien todellisten vastaanottajien tunnisteet kuten verkko- tai laiteosoitteet voidaan ottaa talteen ja simuloida viestinvälitystä mainituille vastaanottajille lisäämällä tunnisteet joko vain ohjelmallisesti tai myös muulla tavoin laitteesta 606 eriytettyyn alilaitteistoon, joka täten osittain vastaa esitetyn turvajärjestelmän alijärjestelmää 2 viestien "välivarastona", jonne laite 606 voi testimielessä välittää vastaanottamansa viestit, mutta joka ei tässä tapauksessa kuitenkaan välitä viestejä oikeasti eteenpäin aidon alijärjestelmän 2 tapaan. Näin ollen myös viestien välitykseen liittyviä virusaktivoitumisen havaitsemiskeinoja voidaan hyödyntää mainitussa laitteessa 606.

Laite sisältää tarvittavan muistin, esim. RAM –muistipiirin 610 ja haihtumattoman muistin 612 kuten kovalevyn tai levykeaseman, ohjelmien, esim. virustentorjunta-ohjelmiston, sisältämien käskyjen tallentamiseksi ja tiedostojen käsittelemiseksi tai tiedostojen käsittelyn simuloimiseksi, sekä suorittimen 614 mainittujen käskyjen toteuttamiseksi. Laite 606 vastaanottaa viestin siihen kytketyltä verkkoelementiltä 602, 604 ja käy viestin lävitse tunnettujen ja tuntemattomien virusten varalta selityksessä jo aikaisemmin mainittuja tekniikoita, mm. kuvion 3 menetelmää, hyödyntäen. Viestin tarkistamisen ajaksi voidaan muu viestinvälitys laitteeseen 606 kytketyssä verkkoelementissä 602, 604 esim. ohjelmallisesti pysäyttää, kunnes laite 606 ilmoittaa mainitulle verkkoelementille 602, 604 viestin olevan puhdas, tai vaihtoehtoisesti voi virushaku olla täysin riippumatonta varsinaisesta viestinvälityksestä muussa järjestelmässä. Vastaavasti myös tarkistettavan viestin välitystä oikealle vastaanottajalleen voidaan viivästyttää, kunnes viesti on todettu laitteen 606 toimesta vapaaksi viruksista. Laite 606 on toisaalta ohjelmoitavissa palauttamaan verkkoelementille 602, 604 tarkistettu viesti kokonaisuudessaankin, jolloin verkkoelementti 602, 604 välittää mainitun tarkistetun viestin sellaisenaan eteenpäin, ja alkuperäinen tarkistamaton kopio viestistä jätetään lähettämättä. Verkkoelementti 602, 604 voidaan vaihtoehtoisesti ohjelmoida hävittämään alkuperäinen viesti heti, kun kopio viestistä on välitetty laitteelle 606 tarkistettavaksi. Täten riski tarkistamattoman viestin kulkeutumisesta eteenpäin saadaan minimoitua.

Laitteen 606 havaitessa välitettävässä viestissä virustartunnan tallentaa se tiedot tapahtuneesta muistiin 610, 612 ja mikäli laitteen 606 ja siihen kytketyn verkkoelementin 602, 604 välinen tiedonsiirtoyhteys on kaksisuuntainen, jossa yhteydessä tiedonsiirtosuunnat voivat olla erotettuna toisistaan, myös edullisesti ilmoittaa viestitse mainitulle verkkoelementille 602, 604 virushälytyksestä. Keksintö on kyseisessä suoritusmuodossaan helppo liittää muuhun, jo toiminnassa olevaan, järjestelmään, koska minimivaatimuksena muun järjestelmän osalta on vain tiedonsiirtoyhteys viestin välittämiseksi varsinaisen kohteen lisäksi myös keksinnön mukaiseen

laitteeseen 606. Lisäksi, esim. ohjelmallisesti toteutettavissa oleva kontrollilogiikka viestinvälityksen pysäyttämiseksi, kunnes laitteelta 606 on vastaanotettu tieto tarkastettavan viestin puhtaudesta, tai vastaavasti virushälytyksen yhteydessä suoritettavat toiminnot, ovat nekin alan ammattimiehelle yksinkertaisia toteuttaa ohjelmallisesti.

Esitetty turvajärjestelmä, menetelmä ja laite virusten torjumiseksi sekä tiedon eristämiseksi pureutuu tietojärjestelmien ja –verkkojen tietoturvan osalta perustavanlaatuiseen ongelmaan; miten ennalta tuntemattomat virukset voidaan havaita ja niiden hyökkäykset torjua. Perinteisesti virus löydetään vasta sen aktivoiduttua kohdejärjestelmässä, minkä jälkeen virus identifioidaan ja löydetyt sormenjäljet lisätään virustentorjuntaohjelmistojen tietokantoihin. Tämä ratkaisutapa edellyttää usealta eri osapuolelta välittömiä toimia, jotta vakavammalta epidemialta vältyttäisiin; viruksen ensimmäisen havaitsijan tulee viipymättä toimittaa saastunut tiedosto tms. virustentorjuntaohjelmiston päivittämisestä vastaavalle taholle, päivittäjän tulee tehdä virustentorjuntaohjelmiston virustietokannasta uusi versio ja toimittaa se jokaiselle käyttäjälle, jonka tulee lopuksi päivittää asiakassovelluksensa tietokanta vastaamaan tehtyjä lisäyksiä. On selvää, että mikäli joku yllä esitetyn tehtäväketjun vaiheista jää tekemättä tai vaihe jostakin muusta syystä, esim. vioittuneiden posti- tai tietoliikenneyhteyksien takia, epäonnistuu, ei viruksen leviämiselle ole esteitä. Ehdotettu uudenlainen ratkaisu tukeutuu aluksi virustietokantaan jo tunnettujen virusten havaitsemista varten, mutta aloittaa sen jälkeen aktivoimisyritykset ja järjestelmän toimintojen yleisen tarkkailun uusien, vielä tuntemattomien viruksien löytämiseksi. Viruksen aktivoituessa vahingot rajoittuvat ennalleen palautettavissa olevaan turvajärjestelmään ja viestiyhteydet sulkeutuvat estäen saastuneiden viestin välittymisen ulkoiseen tai sisäiseen verkkoon. Järjestelmän toimintavarmuutta parannetaan välittämällä suojauskäskyt erillisiä, suojattuja yhteyksiä pitkin. Turvajärjestelmä monitoroi itseään myös silloin, kun varsinaista viestiliikennettä ei ole välitettävänä, jotta mahdollisesti havaitsematta jääneet virukset löytyisivät mahdollisimman varhaisessa vaiheessa. Turvajärjestelmän avulla voidaan erottaa käyttäjän järjestelmä ulkoisesta verkosta tunkeutumisyritysten hankaloittamiseksi.

Edellä esitetyt keksinnön suoritusmuodot ovat vain ei-rajoittavia esimerkkejä ja keksinnön lopullinen toteutus voi täten vaihdella jäljempänä esitettävien patenttivaatimusten sisältämän keksinnöllisen ajatuksen puitteissa.

Viitteet:

[1] The Network Administrators' Guide, URL: http://tldp.org/LDP/nag/, Olaf Kirch 1996

[2] Computer Networks: A Systems Approach, Morgan Kaufmann, ISBN 1-55860-514-2 1999

Patenttivaatimukset

1. Turvajärjestelmä virusten torjumiseksi tietokoneissa ja -verkoissa, joka turvajärjestelmä on järjestetty välittämään viestejä, **tunnettu** siitä, että turvajärjestelmä sisältää ensimmäisen alijärjestelmän (1) tuntemattomien virusten havaitsemiseksi.

2. Patenttivaatimuksen 1 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty välittämään virushavainnon aiheuttama hälytys ainakin yhteen turvajärjestelmään liitettyyn järjestelmään (2, 3).

3. Patenttivaatimuksen 1 tai 2 mukainen turvajärjestelmä, **tunnettu** siitä, että se on virushavainnon aiheuttaman hälytyksen perusteella järjestetty katkaisemaan yhteys ainakin yhteen muuhun järjestelmään (2, 3, 114)

4. Patenttivaatimuksen 1-3 mukainen turvajärjestelmä, **tunnettu** siitä, että se lisäksi sisältää toisen alijärjestelmän (2) viestien välittämiseksi ensimmäisestä alijärjestelmästä (1) ainakin yhteen turvajärjestelmään liitettyyn järjestelmään (3, 210, 114).

5. Patenttivaatimuksen 1-4 mukainen turvajärjestelmä, **tunnettu** siitä, että se lisäksi sisältää kolmannen alijärjestelmän (3), joka on järjestetty hälytyksen vastaanotettuaan katkaisemaan yhteys ainakin yhteen muuhun alijärjestelmään (1,2).

6. Patenttivaatimuksen 5 mukainen turvajärjestelmä, **tunnettu** siitä, että toinen alijärjestelmä (2) sisältää kutakin kolmannen alijärjestelmän (3) laitteen tunnistetta vastaavan tunnisteen.

7. Patenttivaatimuksen 1-6 mukainen turvajärjestelmä, **tunnettu** siitä, että ensimmäinen alijärjestelmä (1) on järjestetty tarkkailemaan toimintojaan virusten havaitsemiseksi.

8. Patenttivaatimuksen 2 mukainen turvajärjestelmä, **tunnettu** siitä, että hälytys on viesti tai ainakin osa viestiä, joka välitetään vastaanottajalle muuta viestiliikennettä nopeammin.

9. Patenttivaatimuksen 5 mukainen turvajärjestelmä, **tunnettu** siitä, että kolmas alijärjestelmä (3) sisältää ainakin yhden tietokoneen tai tietokoneen sisältävän verkkoelementin.

10. Patenttivaatimuksen 2 tai 8 mukainen turvajärjestelmä, **tunnettu** siitä, että hälytys välitetään erillistä yhteyttä pitkin.

11. Patenttivaatimuksen 1-10 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty suorittamaan ainakin yksi toimenpide tuntemattomien virusten aktivoimiseksi.

12. Patenttivaatimuksen 11 mukainen turvajärjestelmä, **tunnettu** siitä, että mainittu toimenpide on yksi seuraavista: aikatiedon muuttaminen, muistin sisällön muuttaminen, tiedostojen käsittely tai ainakin sen osittainen simulointi.

13. Patenttivaatimuksen 1-12 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty vertaamaan ainakin osittain samalla tunnisteella varustettuja viestejä keskenään tuntemattomien virusten havaitsemiseksi.

14. Patenttivaatimuksen 13 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty pyytämään mainittujen samalla tunnisteella varustettujen viestien lähettäjältä ainakin yhtä samalla tunnisteella varustetun viestin uusintalähetystä ja vertaamaan ainakin yhtä vastaanotettua uusintalähetettyä viestiä mainittuihin alkuperäisiin viesteihin viruksia sisältävien viestien havaitsemiseksi.

15. Patenttivaatimuksen 1-14 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty havaitsemaan aktivoitunut virus ainakin yhden seuraavista ehdoista täyttyessä: ensimmäisessä alijärjestelmässä (1) tapahtuu jokin muutos ennen mainitun alijärjestelmän suorittamia muutoksia aiheuttavia toimenpiteitä, ensimmäisessä alijärjestelmässä (1) tapahtuu muutos, joka ei ole mainitun alijärjestelmän viruksen paljastamiseksi tekemä toimenpide, viesti lähtee muuhun järjestelmään ilman ensimmäisen alijärjestelmän (1) käskyä, viesti lähtee muuhun järjestelmään väärään osoitteeseen tai järjestelmään, johon viestiliikennettä ei ole suunnattu, viesti ei lähde muuhun järjestelmään, vaikka se on sinne lähetetty.

16. Patenttivaatimuksen 11 tai 12 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty yhdistämään virusten aktivointikeinoja ajassa joko yhtä aikaa tai peräkkäin tapahtuviksi.

17. Patenttivaatimuksen 11 tai 12 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty valitsemaan virusten aktivointiyrityksissä käytettäväksi logiikaksi ainakin yhden seuraavista: käyttäjän määrittelemä, esiohjelmoitu tai ainakin osittain satunnainen logiikka.

18. Patenttivaatimuksen 5 mukainen turvajärjestelmä, **tunnettu** siitä, että siihen on kytketty kolmannen alijärjestelmän (3) rinnalle järjestelmä, joka on järjestetty tallentamaan kolmannesta alijärjestelmästä (3) lähetetty viesti.

19. Patenttivaatimuksen 18 mukainen turvajärjestelmä, **tunnettu** siitä, että ensimmäinen alijärjestelmä (1) on järjestetty vertaamaan rinnakkaisessa järjestelmässä kolmannesta alijärjestelmästä (3) ensimmäiseen alijärjestelmään (1) lähetetyn ja rinnakkaiseen järjestelmään lisäksi tallennetun viestin viruksen aiheuttaman poikkeavuuden havaitsemiseksi.

20. Patenttivaatimuksen 18 mukainen turvajärjestelmä, **tunnettu** siitä, että mainittu rinnakkainen järjestelmä on järjestetty lähettämään tallentamansa viestin eteenpäin.

21. Patenttivaatimuksen 1-20 mukainen turvajärjestelmä, **tunnettu** siitä, että se on järjestetty tarkastamaan kauttaan välitettävät viestit tunnettujen virusten havaitsemiseksi.

22. Turvajärjestelmä tiedon eristämiseksi ensimmäisen (114) ja toisen (3) järjestelmän välillä, **tunnettu** siitä, että turvajärjestelmä, joka sisältää ensimmäisen (1) ja toisen (2) alijärjestelmän, on järjestetty siirtämään tietoa ensimmäisen (114) ja toisen (3) järjestelmän välillä ensimmäisen (1) ja toisen (2) alijärjestelmän kautta, joka turvajärjestelmä on järjestetty katkaisemaan yhteys ensimmäisen järjestelmän (114) ja ensimmäisen alijärjestelmän (1) välillä ennen yhteyden muodostumista ensimmäisen (1) ja toisen alijärjestelmän (2) välille, ja järjestetty katkaisemaan yhteys ensimmäisen (1) ja toisen (2) alijärjestelmän välillä ennen yhteyden muodostumista toisen alijärjestelmän (2) ja toisen järjestelmän (3) välille.

23. Menetelmä virusten torjumiseksi tietokoneissa ja -verkoissa, **tunnettu** siitä, että se suoritetaan järjestelmässä sisältäen ensimmäisen alijärjestelmän (1) viestien välittämiseksi ja virusten havaitsemiseksi, joka ensimmäinen alijärjestelmä (1) on tiedonsiirron osalta eristettävissä muusta järjestelmästä, joka menetelmä sisältää vaiheet, joissa:

- tarkkaillaan järjestelmän toimintaa viruksen havaitsemiseksi (311),

- havaittaessa virus (312) suoritetaan hälytys (316).

24. Patenttivaatimuksen 23 mukainen menetelmä, **tunnettu** jossa virus havaitaan ainakin yhden seuraavista ehdoista täyttyessä: ensimmäisessä alijärjestelmässä (1) tapahtuu jokin muutos ennen mainitun alijärjestelmän suorittamia muutoksia aiheuttavia toimenpiteitä, ensimmäisessä alijärjestelmässä (1) tapahtuu muutos, joka ei ole mainitun alijärjestelmän viruksen paljastamiseksi tekemä toimenpide, viesti lähtee muuhun järjestelmään ilman ensimmäisen alijärjestelmän (1) käskyä, viesti lähtee

muuhun järjestelmään väärään osoitteeseen tai järjestelmään, johon viestiliikennettä ei ole suunnattu, viesti ei lähde muuhun järjestelmään vaikka se on sinne lähetetty.

25. Menetelmä virusten torjumiseksi tietokoneissa ja -verkoissa, **tunnettu** siitä, että menetelmä sisältää vaiheet, joissa:

- suoritetaan järjestelmässä ainakin yksi toimenpide viruksen aktivoimiseksi (310),

- tarkkaillaan järjestelmän toimintaa virusaktivoitumisen aikaansaaman tapahtuman havaitsemiseksi (311),

- havaittaessa virus (312) suoritetaan hälytys (316).

26. Patenttivaatimuksen 25 mukainen menetelmä, **tunnettu** jossa viruksen aktivoimiseksi suoritettava toimenpide on yksi seuraavista: aikatiedon muuttaminen, muistin sisällön muuttaminen, tiedostojen käsittely tai ainakin sen osittainen simulointi.

27. Patenttivaatimuksen 25 mukainen menetelmä, **tunnettu** joka suoritetaan turvajärjestelmässä käsittäen ensimmäisen alijärjestelmän (1) ja toisen alijärjestelmän (2), jossa menetelmässä virusaktivoituminen havaitaan ainakin yhden seuraavista ehdoista täyttyessä: ensimmäisessä alijärjestelmässä (1) tapahtuu jokin muutos ennen mainitun alijärjestelmän suorittamia muutoksia aiheuttavia toimenpiteitä, ensimmäisessä alijärjestelmässä (1) tapahtuu muutos, joka ei ole mainitun alijärjestelmän viruksen paljastamiseksi tekemä toimenpide, viesti lähtee muuhun järjestelmään ilman ensimmäisen alijärjestelmän (1) käskyä, viesti lähtee muuhun järjestelmään väärään osoitteeseen tai järjestelmään, johon viestiliikennettä ei ole suunnattu, viesti ei lähde muuhun järjestelmään vaikka se on sinne lähetetty.

28. Patenttivaatimuksen 25 mukainen menetelmä, **tunnettu** siitä, että viruksen aktivoimiseksi yhdistetään virusten aktivointikeinoja ajassa joko yhtä aikaa tai peräkkäin tapahtuviksi.

29. Patenttivaatimuksen 25 mukainen menetelmä, **tunnettu** siitä, että virusten aktivointiyrityksissä käytettäväksi logiikaksi valitaan ainakin yksi seuraavista: käyttäjän määrittelemä, esiohjelmoitu tai ainakin osittain satunnainen logiikka.

30. Patenttivaatimuksen 25 mukainen menetelmä, **tunnettu** siitä, että se lisäksi sisältää vaiheen, jossa etsitään tunnettuja viruksia (306) niille ominaisten tuntomerkkien avulla.

31. Menetelmä tiedon eristämiseksi ensimmäisen (114) ja toisen (3) järjestelmän välillä, **tunnettu** siitä, että menetelmä suoritetaan turvajärjestelmässä, joka sisältää ensimmäisen (1) ja toisen (2) alijärjestelmän, joiden alijärjestelmien (1, 2) kautta siirretään tietoa ensimmäisen (114) ja toisen (3) järjestelmän välillä, joka menetelmä sisältää vaiheet, joissa:

- katkaistaan yhteys ensimmäisen järjestelmän (114) ja ensimmäisen alijärjestelmän (1) välillä,

- muodostetaan yhteys ensimmäisen alijärjestelmän (1) ja toisen alijärjestelmän (2) välille,

- katkaistaan yhteys ensimmäisen alijärjestelmän (1) ja toisen alijärjestelmän (2) välillä,

- muodostetaan yhteys toisen alijärjestelmän (2) ja toisen järjestelmän välille (3).

32. Laite virusten torjumiseksi tietokoneissa ja -verkoissa, joka laite sisältää välineet tiedon tallentamiseksi (610, 612) ja käsittelemiseksi (614) sekä välineet tiedon siirtämiseksi (608) toisen laitteen kanssa, **tunnettu** siitä, että laite on järjestetty vastaanottamaan viesti mainitulta toiselta laitteelta ja tarkistamaan mainittu viesti tuntemattomien virusten havaitsemiseksi.

33. Patenttivaatimuksen 32 mukainen laite, **tunnettu** siitä, että se on järjestetty suorittamaan ainakin yksi toimenpide tuntemattomien virusten aktivoimiseksi.

34. Patenttivaatimuksen 33 mukainen laite, **tunnettu** siitä, että mainittu toimenpide on ainakin yksi seuraavista: aikatiedon muuttaminen, muistin sisällön muuttaminen, tiedostojen käsittely tai ainakin sen osittainen simulointi.

35. Patenttivaatimuksen 32-34 mukainen laite, **tunnettu** siitä, että se on järjestetty havaitsemaan virusaktivoituminen ainakin yhden seuraavista ehdoista täyttyessä: tapahtuu muutos ennen laitteen tekemiä muutoksia aiheuttamia toimenpiteitä, tapahtuu muutos, joka ei ole laitteen viruksen paljastamiseksi tekemä toimenpide,

36. Patenttivaatimuksen 32-35 mukainen laite, **tunnettu** siitä, että se on järjestetty lähettämään viesti joko laitteen osalaitteistolle tai mainitulle toiselle laitteelle, ja järjestetty havaitsemaan virusaktivoituminen ainakin yhden seuraavista ehdoista täyttyessä: viesti lähtee ilman laitteen virustentorjuntaohjelmiston hyväksyntää, viesti lähtee osoitteeseen, johon sitä ei ole alun perin suunnattu, viesti ei lähde vaikka sille on annettu lähetyskäsky.

37. Patenttivaatimuksen 33 mukainen laite, **tunnettu** siitä, että se on järjestetty yhdistämään virusten aktivointikeinoja ajassa joko yhtä aikaa tai peräkkäin tapahtuviksi

38. Patenttivaatimuksen 33 mukainen laite, **tunnettu** siitä, että on järjestetty valitsemaan viruksen aktivointiyrityksessä käytettäväksi logiikaksi ainakin yhden seuraavista: käyttäjän määrittelemä, esiohjelmoitu tai ainakin osittain satunnainen logiikka.

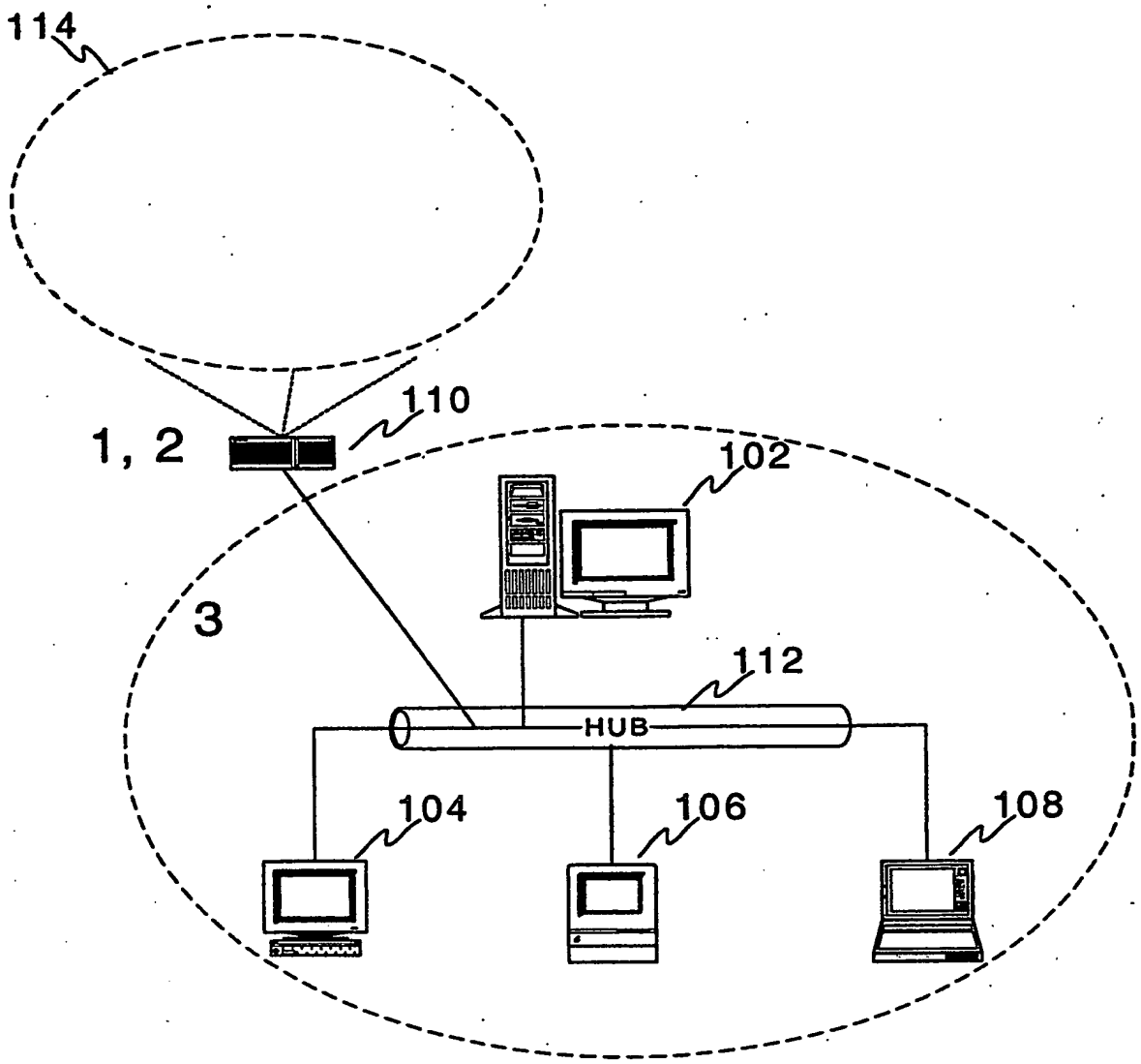
39. Patenttivaatimuksen 32-38 mukainen laite, **tunnettu** siitä, että se on järjestetty tarkastamaan mainittu viesti tunnettujen virusten havaitsemiseksi.

40. Patenttivaatimuksen 32-39 mukainen laite, **tunnettu** siitä, että se on järjestetty tarkkailemaan toimintojaan virusten havaitsemiseksi.

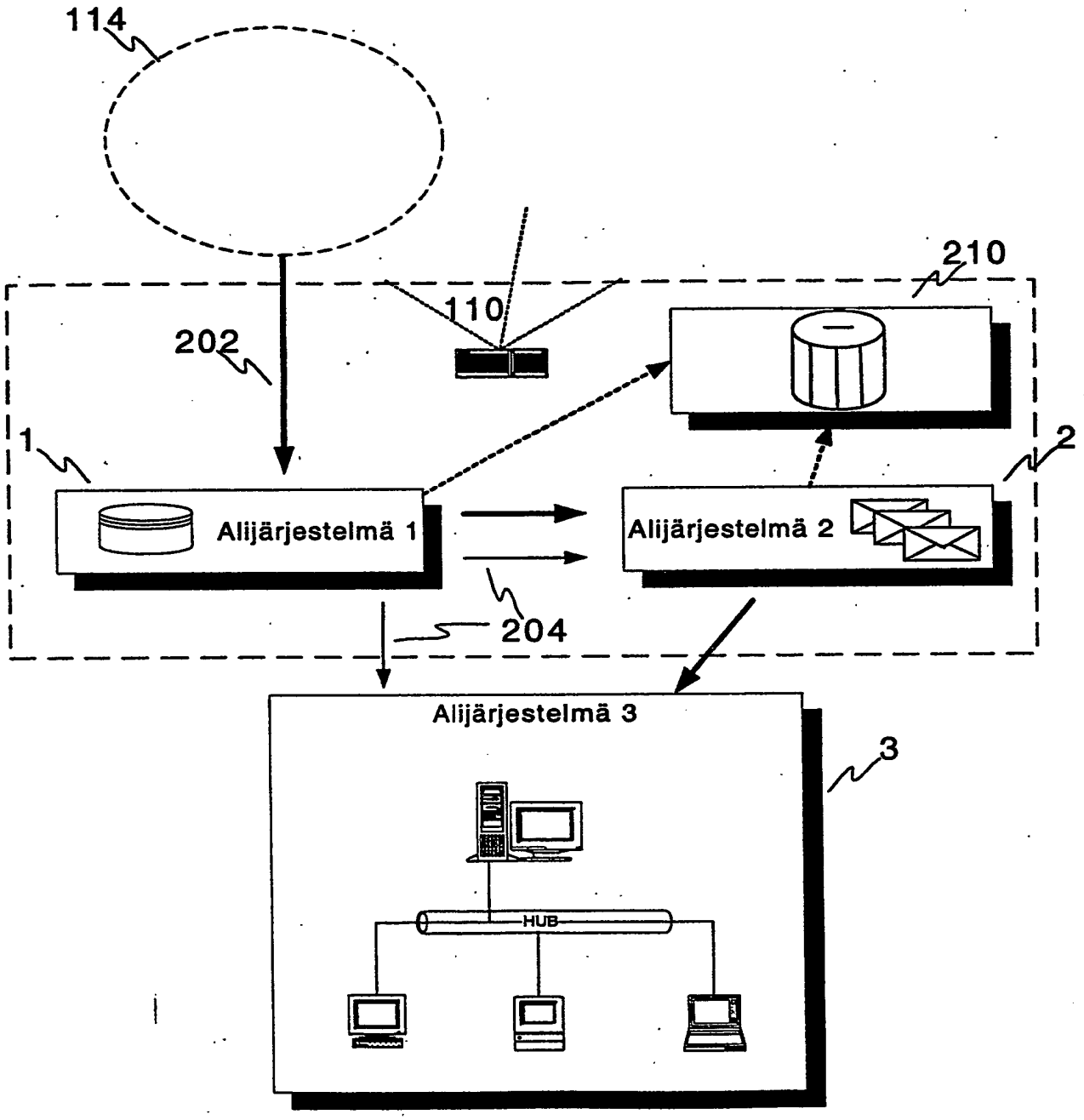
(57) Tiivistelmä

Keksinnön kohteena on turvajärjestelmä, menetelmä ja laite virusten torjumiseksi sekä tiedon eristämiseksi. Turvajärjestelmä käsittää alijärjestelmät 1-3, joka alijärjestelmä 1 sisältää virustorjuntaohjelmiston lisäksi ne alijärjestelmän 3 ohjelmat, jotka voivat aikaansaada viruksen aktivoitumisen. Alijärjestelmä 2 toimii viestiliikenteen väliportaana alijärjestelmien 1 ja 3 välillä. Esitetyssä menetelmässä suoritetaan toimenpiteitä viruksen aktivoimiseksi ja virusaktivoitumisen havaitsemiseksi. Virusaktivoitumisen yhteydessä turvajärjestelmä tai sen osa voidaan erottaa muusta järjestelmästä ja siten rajoittaa syntyviä vahinkoja. Kun turvajärjestelmä sijoitetaan kahden järjestelmän väliin, voidaan sitä käyttää myös eristämään mainitut kaksi järjestelmää toisistaan suoran, reaaliaikaisen tiedonsiirron osalta. Keksinnön mukainen laite on järjestetty vastaanottamaan viesti toiselta laitteelta ja tarkistamaan mainittu viesti tuntemattomien virusten aktivoimiseksi ja havaitsemiseksi.

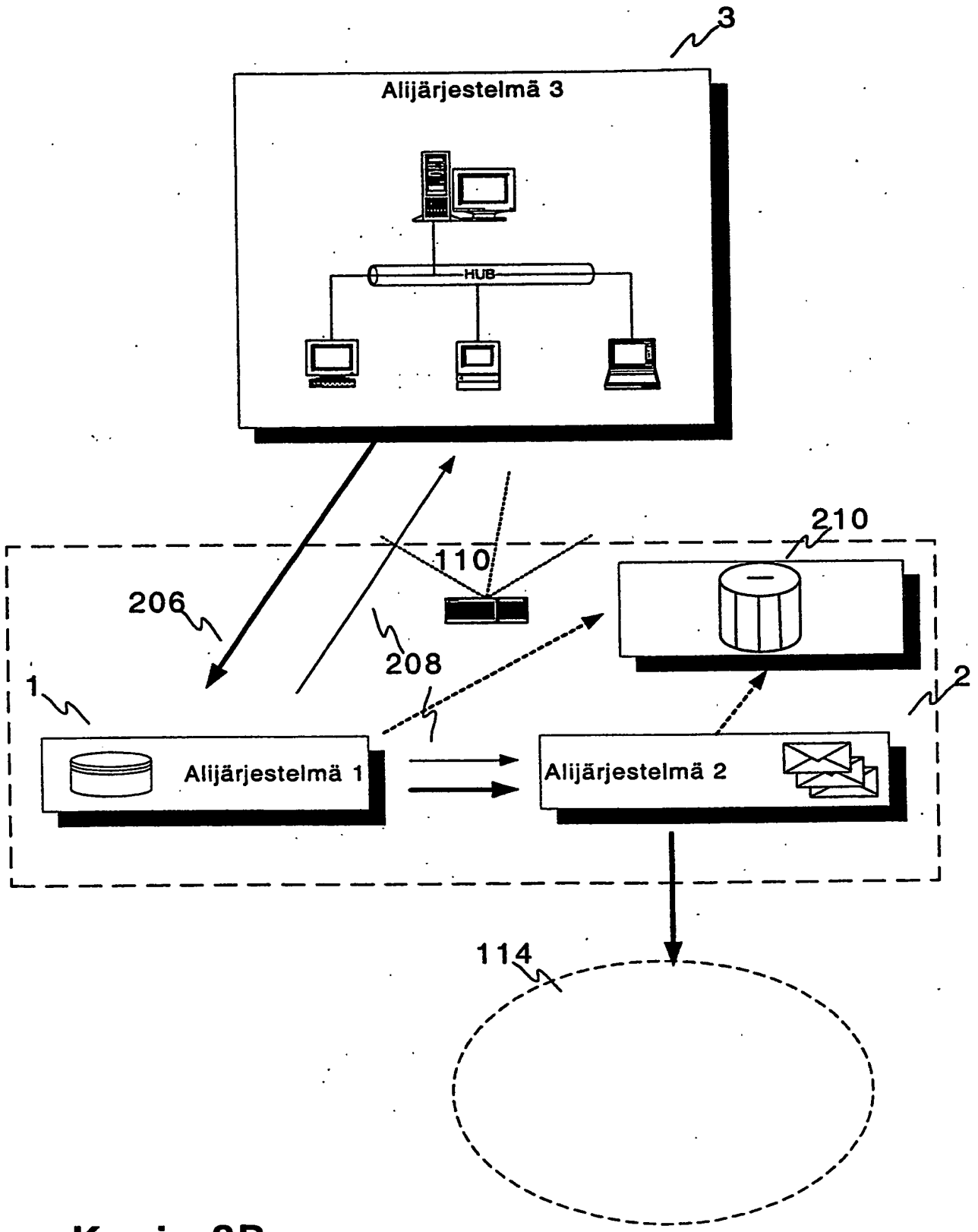
Kuvio 2A



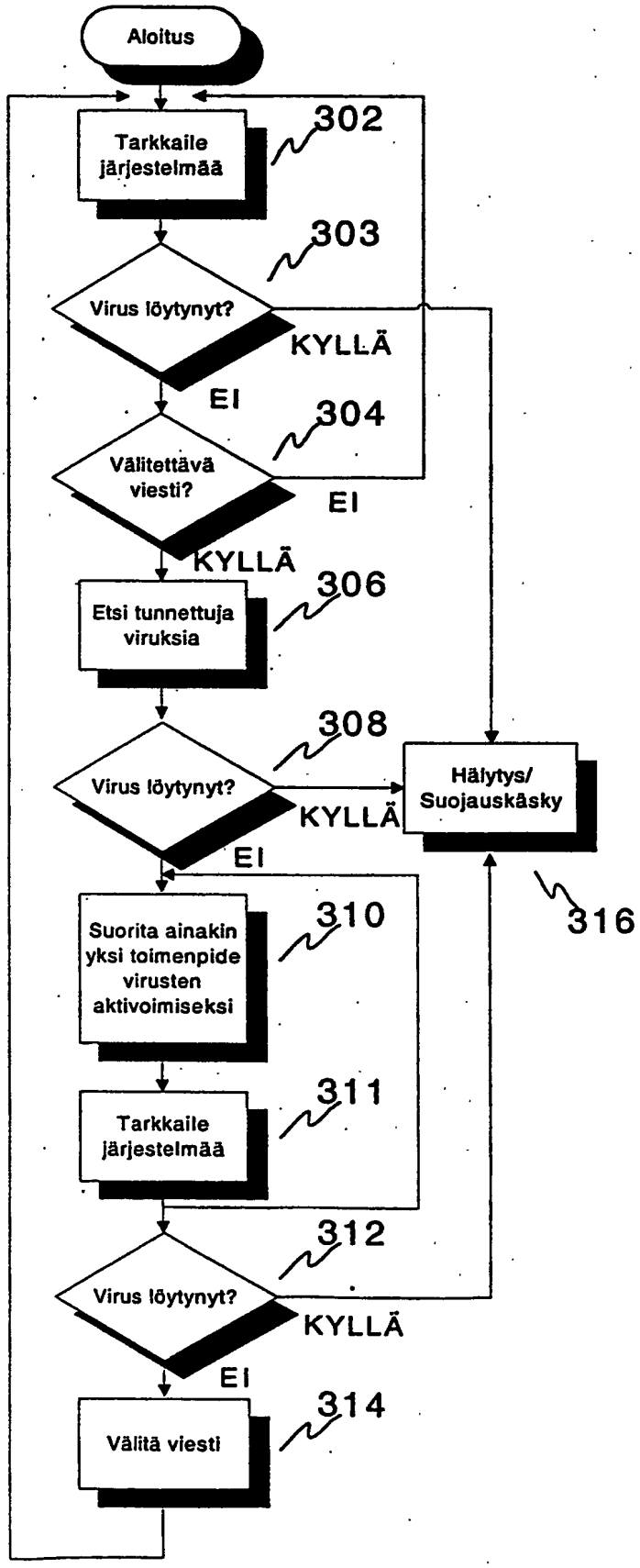
Kuvio 1


114
210
110
202
1
2
Alijärjestelmä 1
Alijärjestelmä 2
204
Alijärjestelmä 3
3
HUB

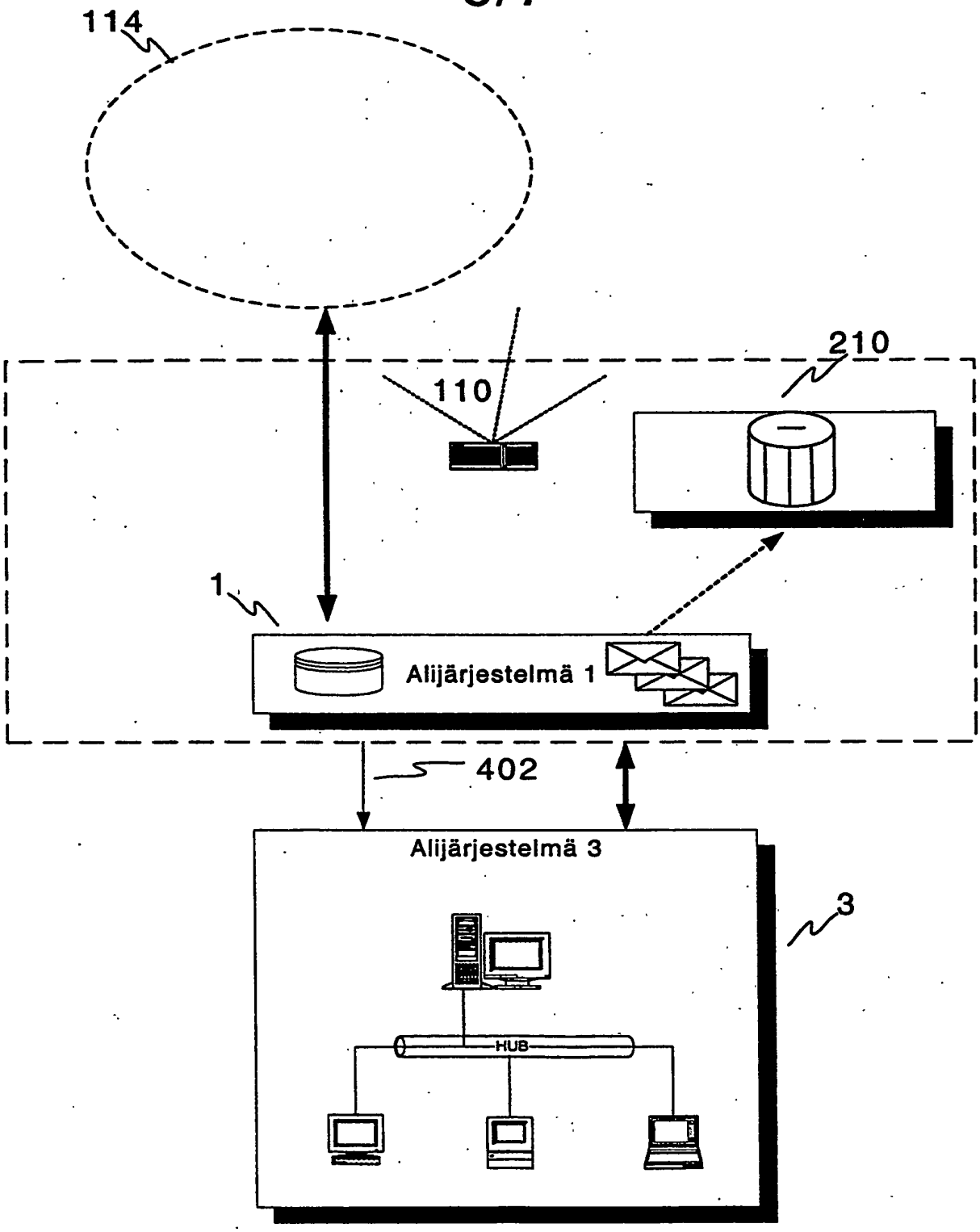
Kuvio 2A


3
Alijärjestelmä 3
HUB
210
110
206
208
1
2
Alijärjestelmä 1
Alijärjestelmä 2
114

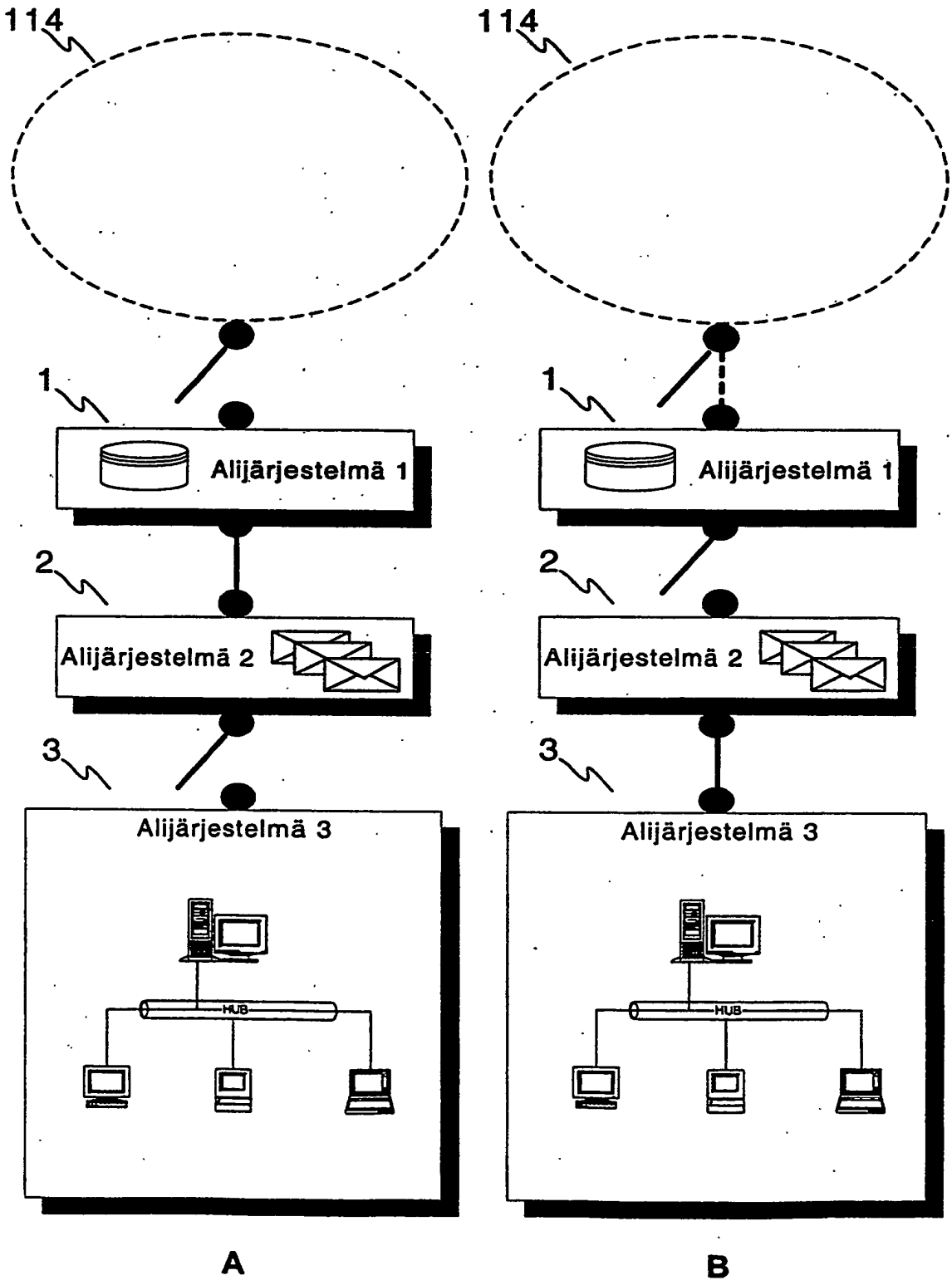
Kuvio 2B


Aloitus
Tarkkaile järjestelmää
302
Virus löytynyt?
303
KYLLÄ
EI
Välitettävä viesti?
304
EI
KYLLÄ
Etsi tunnettuja viruksia
306
Virus löytynyt?
308
KYLLÄ
EI
Hälytys/ Suojauskäsky
316
Suorita ainakin yksi toimenpide virusten aktivoimiseksi
310
Tarkkaile järjestelmää
311
Virus löytynyt?
312
KYLLÄ
EI
Välitä viesti
314

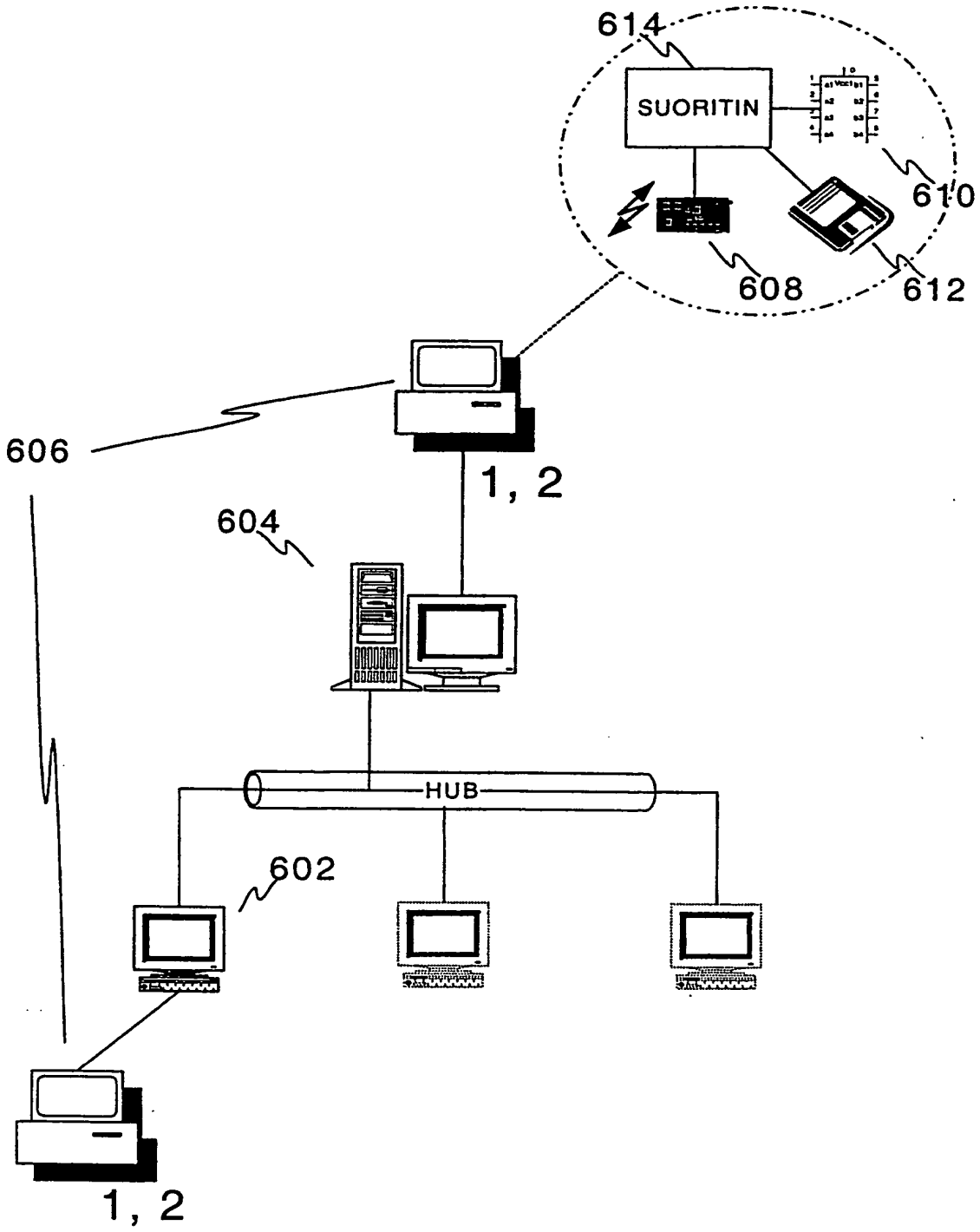
Kuvio 3



Kuvio 4


114
114
1
1
Alijärjestelmä 1
Alijärjestelmä 1
2
2
Alijärjestelmä 2
Alijärjestelmä 2
3
3
Alijärjestelmä 3
Alijärjestelmä 3
HUB
HUB
A
B

Kuvio 5



Kuvio 6